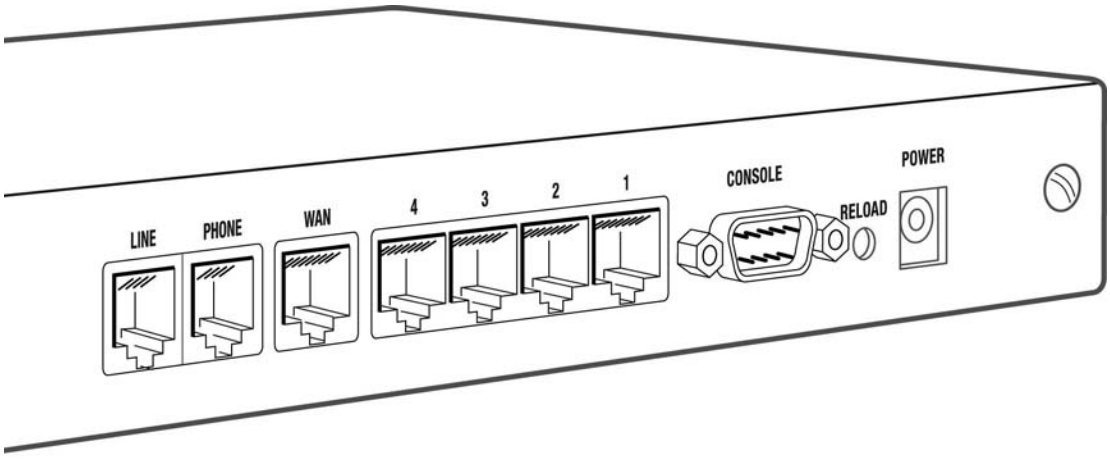
BSGX4e
Business Gateway
User Guide

Release 01.01



Trademarks

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks appearing in this guide are the exclusive property of their respective owners.

Hardware Notice

WARNING: Before working on this equipment, be aware of good safety practices and the hazards involved with electrical circuits.

WARNING: To reduce risk of injury, fire hazard, and electric shock, do not install the unit near a damp location.

CAUTION: Do not connect the FXS port (labeled PHONE) to the central office line.

CAUTION: To reduce the risk of fire, use only number 26 AWG or larger UL Listed or CSA Certified telecommunication line cord for all network and telecommunication connections.

CONTENTS

ABOUT THIS GUIDE

Audience 23
Organization 23
Conventions 25
  Command Prompt Convention 25
  Text Font Conventions 25
Documentation 26
How to get help 26
  Getting Help from the Nortel Web site 26
  Getting Help over the phone from a Nortel Solutions Center 26
  Getting Help from a specialist by using an Express Routing Code 27
  Getting Help through a Nortel distributor or reseller 27

1 CONNECTING TO THE DEVICE

Network Role 29
Device Features 30
Connecting to the Unit 32
  Finding an IP Address using a Console Session 32
  Remote Administration Services 33
Telnet Access 34
  Telnet Configuration Command 34
  Telnet Configuration Example 35
  Show Telnet Configuration 35
  Telnet Client Command 35
  Telnet Session Example 35
SSH Server 36
  Digital Signature Algorithm (DSA) Host Keys 36
  SSH Configuration Command 36
  SSH Example 37
  Show SSH Configuration 37
  Regenerate SSH keys 37
  Upload Public Key 38
Web Server 38
  Web Server Configuration Command 39
  Disable Web Server Example 39
  Show Web Server Configuration 39
  Show Web Server Statistics 40
SSL 40
  SSL Key 40
  SSL CSR 41
  SSL Certificate 42
  SSL Configuration Example 43
  Show SSL Configuration 43

2 INITIAL SETUP

Setting the Time 47
Show the Current Time 47
Setting the Time Manually 47
Setting the Time through an SNTP Server 48
Watchdog Reset Timer 49
Watchdog Timer Command 49
Watchdog Timer Example 50
Show Watchdog Configuration 50
DNS Client 50
DNS Client Configuration Command 50
DNS Client Configuration Example 51
Show DNS Client Configuration 52
Check DNS Server Accessibility 52
Initial Settings 52

3 USER MANAGEMENT

User Management Features 57
Password Entry 58
Failed log on Attempts 58
Changing a Password 59
Showing Active Users 60
User Accounts, Groups and Rights 61
User Configuration Commands 61
User Accounts 61
Add User Account Example 63
Show User Account 63
Deleting a User Account 63
User Groups 64
Add User Group Example 65
Show a User Group 65
Deleting a User Group 65
User Rights 66
Command Authority 66
Configuration Requirements 66
Configuration Command 67
Add User Rights Example 67
Show User Rights Record 68
Deleting a User Rights Record 68
Radius Authentication 68
Configuration Requirements 69
Configuration Steps 69
Radius Authentication Records 69
Example of Configuring a Radius Authentication Record 70
Show Radius Authentication Records 71
Radius Activity Logs 71
TACACS+ Authentication 71
Configuration Steps 72

TACACS+ Authentication Records 72
Example of Configuring a TACACS+ Authentication Record 73
Show TACACS+ Authentication Records 73
TACACS+ Activity Logs 74
TACACS+ Authentication 74
Configuration Requirements 74
TACACS+ Authentication Records 75
Example of Configuring a TACACS+ Authentication Record 75

4 COMMAND INTERFACE

Command Entry 77
Logging Off 78
Exit Command 78
Customizing the Command Session 78
Changing the Terminal Settings 79
Saving Configuration Changes 79
Showing the Configuration 80
Defining Auto Run Commands 80
Online Help 81
General Help 81
Specific Help 81
Interactive Mode 82
CLI Command Syntax 83
Parameter Values 84
Command Keyword NO 84
Command Keyword ALL 85
Maintenance Commands 86
Maintenance Command Syntax 86
Maintenance Command Help 86
List of Maintenance Commands 86
Debug Commands 88
Debug Command Syntax 88
Debug Command Help 88
List of Debug Commands 88

5 WAN INTERFACE CONFIGURATION

Ethernet WAN Port and Interface 91
WAN Ports 91
WAN Interface (eth0) 92
eth0 Configuration Command 92
Show eth0 Configuration 94
eth0 Statistics 94

6 LAN SWITCH CONFIGURATION

Introduction 97
LAN Switch Ports 97
LAN Port Configuration Command 98
LAN Port Configuration Examples 98

Show Port Configuration 99
Show Port Status 99
Show Port Statistics 100
LAN Interface (eth1) 102
eth1 Configuration Command 102
Configure eth1 Interface Example 102
Show eth1 Configuration 103
ARL Configuration 104
ARL Configuration Command 104
Show ARL Table 105
Remove an ARL Entry 106
Flush ARL Table 106
Layer 2 QoS 106
Priority Queues 107
Selecting Layer 2 QoS Settings 108
Mapping Port Numbers to Priority Queues 108
Mapping IEEE 802.1p Tags to Priority Queues 108
Mapping ToS/DiffServ Tags to Priority Queues 109
Layer 2 QoS Configuration Example 109
Show Layer 2 QoS Configuration 109

7 VLAN CONFIGURATION

Assigning Ports to a VLAN 111
Packet Tagging 112
VLAN Port Assignment Command 112
VLAN Port Assignment Examples 112
Show VLAN Port Assignments 113
Delete VLAN Port Assignment 113
Configuring a VLAN Interface 114
Configuration Constraints 114
Virtual Interface Configuration 114
VLAN IP Address Assignment 115
Virtual Interface Configuration Examples 116
Modifying or Deleting a VLAN 117

8 ROUTING CONFIGURATION

Introduction 121
Configuring ARP 122
ARP Entry Configuration Command 122
ARP Entry Example 122
Show ARP Table 122
Delete ARP Entry 123
Flush ARP Table 123
Protecting ARP Traffic 123
Configuring Static Routes 124
Route Configuration Command 124
Static Route Examples 125
Show Route Table 125

Delete a Static Route 126
Starting the RIP Daemon 126
RIP Constraints 126
RIP Daemon Command 126
RIP Daemon Example 127
Show RIP Status 127
Show RIP Routes 127

9 SECURITY CONFIGURATION

Secure Traffic Processing 129
Firewall Security Policies 130
Initial Firewall Security Policies 130
Configuration Constraints 130
Security Policy Sequence 130
Security Policy Configuration Command 131
Firewall Security Policy Example 132
Show Firewall Security Policies 132
Remove a Firewall Security Policy 132
Show Firewall Log Entries 132
Connection Time-outs 133
Connection Timeout Command 133
Show Timeout Settings 133
NAT/ALG 134
Configuring NAT 134
Enable NAT on the WAN Interface 135
Configuring NAT Policies 135
Configuring NAT Public Addresses 136
Port Forwarding 137
Address Forwarding 138
Static NAT Forwarding 138
Show NAT Policies 139
ALG Configuration 140
IDS 140
Attack Types 141
Packet Anomaly Protection 141
Flood Protection 143
Scan Protection 146
Spoof Protection 147
IDS Statistics 149
Clear IDS Statistics 150
Show IDS Log Entries 150

10 VPN CONFIGURATION

VPN Support 153
IKE 154
IKE Policies 155
IKE Lifetime Parameters 155
IKE Preshared Key Records 156

Show IKE Security Associations 157
Show IKE Statistics 158
IPsec 158
IPsec Parameters 159
IPsec Proposals 160
IPsec Policies 160
Show IPsec Security Associations 162
IPsec Statistics 163
VPN Configuration Examples 163
Office-to-Office VPN Example 163
ISP Tunnel Example 166
Configuring a VPN 169
VPN support on BSGX4e 174
Example 175
Configuration of BSGX4e using a single tunnel 175
Configuration of Cisco 176
Troubleshooting on BSGX4e 177

11 GoS Configuration

Introduction to GoS 181
Quality Groups 182
GoS Classes 182
Traffic Policing 183
Configuring GoS 185
Configuring a GoS Link 186
GoS Link Example 186
Show the GoS Link 186
Delete GoS Link 187
Configuring Quality Groups 187
Configuration Constraints 187
Downgraded and Dropped Packets 187
Default Best Effort Quality Group 188
Quality Group Command 188
Quality Group Examples 189
Show Quality Groups 190
Delete a Quality Group 190
Assigning Traffic Flows to Quality Groups 190
VoIP Traffic Protection 191
ARP Traffic Protection 191
Traffic Protection by Security Policy 191
GoS Security Policy Examples 192
Show GoS Security Policies 193
Delete a Security Policy 193
GoS Statistics 193
Cumulative Statistics 193
Clearing GoS Cumulative Statistics 195
Instantaneous Statistics 195
Configuring QoS 197
Example 200

Configuring Layer 2 QoS 201
Configuring Layer 3 QoS 204

12 MGCP CONFIGURATION

Introduction to MGCP 209
MGCP Session Controller 210
MGCP Gateway 211
MGCP Configuration Steps 211
MGCP Call Servers 212
Call Server Failover 212
MGCP Server Profile Command 213
MGCP Server Profile Examples 213
Show Server Settings 214
Delete MGCP Server Profile 214
Show MGCP Server Status 214
MGCP Session Controller Configuration 215
MGCP Signaling Proxy (MSP) 216
Endpoint Status Handling (ESH) 220
MGCP Gateway 222
Configuring MGCP Settings for the Gateway 222
Configuring the MGCP Gateway 223
MGCP Endpoints 227
Preparing Endpoints for Registration 227
Verify Endpoint Registration 228

13 VOIP CONFIGURATION

Media Bridge (MBR) 229
Media Settings Command 229
Media Settings Example 230
Show Media Settings 230
Show Media Status 230
Show Media Connection Statistics 231
Access Control List (ACL) 232
Access Control List Command 233
ACL Entry Example 233
Show ACL 234
Cisco Discovery Protocol (CDP) 234
Show CDP Entry 234
Show CDP Neighbors 235
Show CDP Statistics 236
Call Admission Control (CAC) 236
VoIP Bandwidth Requirements 236
Show Call Admission Settings 237
FXS Port Configuration 238
Country Code and Unit Name Setting 239
Jitter Buffer Settings 240
Call Progress Tones 241
DSP Gain Settings 243

Line Impedance Settings 243
Electrical Status 244
Line Fault Testing 245
Voice Quality Monitoring (VQM) 247
Monitored Calls 248
VQM Analyser Command 249
VQM Analyser Example 250
Show VQM Analyser Configuration 250
Show VQM Call Summary 250
Voice Quality Statistics 251
Alarm Log Entries 252
Alarm Statistics 252
Call Records 253
Show Current Calls 253
Show Call History 254

14 LOCAL CALL ROUTING

VoIP Service Interruption 255
Local Call Routing (LCR) Mode 256
LCR Configuration 256
LCR Account Configuration 256
LCR Settings 257
FxO Gain and Impedance Settings 259
Show LCR Status 262
Show LCR Connections 262

15 SIP CONFIGURATION

Introduction to SIP 263
SIP Session Controller 264
SIP Gateway 265
SIP Configuration Steps 265
SIP Call Server Access 266
Call Server Failover 266
Additional Inbound Servers 266
SIP Server Profile Command 267
SIP Server Profile Examples 267
Show SIP Server Settings 269
Delete SIP Server Profile 270
Show SIP Server Status 270
SIP Session Controller 271
SIP Signaling Proxy (SSP) 272
Session Controller Setting Command 272
Show SIP Session Controller Settings 273
Show SIP Session Controller Status 274
Show SIP Signaling Statistics 274
Show SIP Call Statistics 275
Show SIP Call Records 276
Show Registered Endpoints 276

Endpoint Status Handling (ESH) 277
SIP Gateway 278
SIP Settings for the Gateway 278
SIP Gateway Configuration 280
Numbering Plan for the Gateway 284
SIP Endpoints 288
Preparing Endpoints for Registration 288
Verify Endpoint Registration 289
IP Address Change 289
Configuring SIP 290
Step 1-Configure BSGX4e Session Controller 292
Configuration of the IP Network 292
Data service configuration for the LAN VoIP phones: DHCP, SNTP, and TFTP296
Configuration of the SIP voice services offered to LAN VoIP phones .. 297
Step 2-Configuring the BSGX4e User Agent 299
Step 3-Configure LAN VoIP phones (Example using Cisco 7960) 300
Step 4-Check the overall configuration 301
Step 5-Make calls 302
Annex A-Configuration example for Cisco 7960 SIP phone 303
Annex B-Call Admission Controller algorithm 306

16 VoIP Services and Relays

DHCP Server 309
Default DHCP Server Configuration 309
DHCP Server Configuration Command 310
DHCP Server Configuration Example 311
Show DHCP Server Configuration 311
Show DHCP Leases 312
DHCP Relay 312
DHCP Relay Command 312
DHCP Relay Example 313
Show DHCP Relay Settings 313
DNS Relay 313
DNS Relay Command 313
DNS Relay Example 314
Show DNS Relay Settings 314
Show DNS Sessions 314
Show DNS Relay Cache 314
SNTP Relay 315
SNTP Relay Command 315
SNTP Relay Example 315
Show SNTP Settings 316
Show SNTP Sessions 316
TFTP Relay 316
TFTP Relay Command 316
TFTP Relay Settings Example 317
Show TFTP Relay Settings 317
Show TFTP Sessions 317
TFTP File Cache 318

TFTP Cache Command 318
Specifying Files to be Cached 318
TFTP Cache Example 319
Show TFTP Cache Settings and Usage 319
Show TFTP Cache Contents....319
Delete Files to be Cached 320
Clear TFTP Cache 320

17 MONITORING

Show System Exceptions 321
Show Hardware Information 322
Show System Status 322
Show System Operation Summary 323
Audit Logging 324
Audit Log Command 324
Show Audit Log Status 324
Show Audit Log Entries 325
Clear Audit Log 325
Module Logging 325
Logging Level Command 326
Mapping Log Destinations 327
Show Module Log Entries....329
Configure Log Server 329
Ethernet Interface Statistics 331
IP Stack Statistics 331
IP Statistics 332
ICMP Statistics 333
UDP Statistics 335
TCP Statistics 335

18 MONITORING TOOLS

Port Mirroring 339
Port Mirroring Constraints 339
Port Mirroring Command 339
Mirroring Configuration Example 340
Show Mirroring Configuration 340
Deleting a Port Mirroring Entry 340
Protocol Monitoring (PMON) 340
Enable PMON Command 341
PMON Trace Command 341
PMON Configuration Example 342
Show PMON Status 342
Show PMON Traces 342
Show PMON Trace Statistics 343
Clear PMON Trace Statistics 343
Netflow Exporter 343
Netflow Exporter Command 344
Netflow Filter Command 345

Netflow Configuration Example 345
Show Netflow Status 346
Show Netflow Filters 346
Show Netflow Statistics 346
Clear Netflow Statistics 346
SNMP Agent 347
SNMP Configuration Command 347
SNMP Community Command 348
SNMP Agent Configuration Example 348
Show SNMP Agent Configuration 349
Show SNMP Community Configuration 349
Show SNMP Agent Statistics 349
Clear SNMP Statistics 351
SNMP Traps 351
Copying Trap MIB Data 352
TCPdump Command 352
TCPDump Command Options 352
Limited Capture Example 354
Ping Command 355
Ping Example 356
Traceroute Command 356
Traceroute Example 357

19 SOFTWARE UPGRADES

File System 359
File System Navigation 359
File System Management 360
Software Upgrade Procedures 362
Device Software 362
Check Current Software Versions 362
Web UI Upgrade Procedure 363
Requirements 363
Save the Current Configuration 363
Upgrade Software through Web UI 365
Change Default Application Image 368
View Bootloader Version 369
Restore the Configuration 369
SFTP Upgrade Procedure 371
Listing the Configuration 374

A WEB USER INTERFACE

..... 379
Web UI Features 380
Logging on to the Web UI 380
Access Requirements 381
Log on Procedure 381
Web UI Screen Structure 382
Menus 382

Help Icons 382
Operations Menu 383
Web UI Menus 384
Configuration Example 388
Monitoring Example 390
Wizards Example 391
Exit Web UI 396

B THIRD PARTY SOFTWARE

Software Applications 399

C SSH FUNCTIONALITY

Introduction 401
SSH Server Functionality 401
SFTP 402
Authentication 402
Host Keys 403
Remote Log on 403
Service Functions 403
SSH Service 403
SFTP Service 404
SSH System Architecture 404
SSH-TRANS 404
SSH-AUTH 405
SSH-CONNECTION 405

D TCPDUMP EXPRESSIONS

Introduction 407
Expressions 407
Primitives 407

E STANDARDS COMPLIANCE

Data Standards 411
Switching 411
Routing 411
Security 412
Quality of Service 412
Services 413
Monitoring 413
Voice Standards 414
SIP Session Controller 414
MGCP Session Controller 415
SIP User Agent (Integrated Gateway) 415
MGCP User Agent (Integrated Gateway) 416

F RULE COMPLIANCE

FCC Compliance (U.S.) 419

FCC Telecom Statement 419
Declaration of Conformity 420
Equipment Attachment Regulations (Canada) 421
Canadian Department of Communications Statement 421
Supplementary Information 421

G COPYRIGHT INFORMATION

..... 423

H GLOSSARY

..... 429

INDEX

..... 433

TABLES

1 User Guide Organization 23
2 Text Conventions 25
3 Telnet Server Configuration Parameters 35
4 Telnet Parameters 35
5 SSH Configuration Parameters 37
6 Web Server Configuration Parameters 39
7 Web Server Statistics 40
8 SSL Key Configuration Parameters 41
9 SSL CSR Configuration Parameters 41
10 SSL Certificate Configuration Parameters 43
11 SNTP Server Configuration Parameters 48
12 System Watchdog Configuration Parameters 49
13 DNS Client Configuration Parameters 51
14 Initial Settings 53
15 Config User Commands 61
16 User Account Configuration Parameters 62
17 User Group Configuration Parameters 64
18 User Rights Parameters 67
19 Radius Authentication Record Parameters 70
20 TACACS+ Authentication Record Parameters 73
21 TACACS+ Authentication Record Parameters 75
22 Terminal Session Parameters 79
23 Autorun Command Parameters 80
24 eth0 Parameters 92
25 LAN Port Parameters 98
26 LAN Port Summary Statistics 100
27 LAN Interface Parameters 102
28 ARL Parameters 104
29 Default Priority Queues 107
30 Layer 2 QoS Setting Parameters 108
31 Layer 2 QoS Port Mapping Parameters 108
32 Layer 2 QoS 802.1p Tag Mapping Parameters 108
33 Layer 2 QoS DiffServ/ToS Mapping Parameters 109
34 VLAN Configuration Parameters 112
35 Virtual Interface Parameters 114
36 IP Address Assignment Parameters 115
37 ARP Route Parameters 122
38 Route Configuration Parameters 125
39 RIP Daemon Parameters 127
40 Traffic Classification 129

41 Security Policy Parameters 131
42 Connection Configuration Parameters 133
43 NAT Status Parameters 135
44 NAT Policy Configuration Parameters 136
45 ALG Configuration Parameters 140
46 Protocols to which IDS Attack Protection Applies 141
47 Packet Anomaly Attacks 142
48 Packet Fragment Anomaly Parameters 142
49 Flood Detection Activation Parameters 144
50 Default Flood Threshold Values 145
51 Flood Threshold Setting Parameters 146
52 IDS Scan Configuration Parameters 147
53 Default Trust Settings for Interfaces 148
54 IDS Spoof Configuration Parameters 148
55 IKE Parameters 155
56 IKE Preshared Configuration Parameters 156
57 IKE SAs 158
58 IPsec Parameters 159
59 IPsec Proposal Parameters 160
60 IPsec Policy Parameters 161
61 Network information 169
62 Performance of each module with QoS running concurrently 171
63 ESP Statistics 179
64 GoS Link Configuration Parameters 186
65 GoS Group Configuration Parameters 188
66 GoS Cumulative Statistics 194
67 GoS Instantaneous Statistics 196
68 Network Information 197
69 Server Information 197
70 MGCP Server Profile Parameters 213
71 MGCP Session Controller Parameters 216
72 MGCP Gateway Parameters 223
73 MGCP Gateway Configuration Parameters 224
74 Media Stream Parameters 230
75 Voice ACL Parameters 233
76 System Info Parameters 239
77 Voice Jitter Buffer Configuration Parameters 240
78 Call Progress Tone Parameters 242
79 Call Analyser Configuration Parameters 249
80 Call Record Fields 253
81 LCR Account Parameters 257
82 LCR Configuration Parameters 258

83 AC Impedance Register Values 261
84 SIP Server Profile Parameters 267
85 SIP Session Controller Parameters 273
86 SIP Gateway Parameters 279
87 SIP Gateway Configuration Parameters 281
88 SIP Numbering Plan Parameters 284
89 Network Information 291
90 Server Information 291
91 DHCP Server Configuration Parameters 310
92 DHCP Relay Parameters 312
93 DNS Relay Parameters 314
94 SNTP Relay Configuration Parameters 315
95 TFTP Relay Configuration Parameters 316
96 TFTP Cache Configuration Parameters 318
97 TFTP Files Configuration Parameters 319
98 System Exception Information Fields 321
99 Message Severity 326
100 Logging Modules Configuration Parameters 326
101 Log Destination Map Parameters 328
102 Log Server Parameters 330
103 IP Statistics 332
104 ICMP Statistics 334
105 UDP Statistics 335
106 TCP Statistics 336
107 Mirroring Parameters 340
108 PMON Trace Parameters 342
109 Netflow Agent Configuration Parameters 344
110 Netflow Filter Configuration Parameters 345
111 SNMP Agent Configuration Parameters 347
112 SNMP Community Configuration Parameters 348
113 SNMP Data Fields 349
114 SNMP Agent Statistics 350
115 SNMP Traps Configuration Parameters 351
116 TCPDump Options 353
117 Ping Options 355
118 Traceroute Options 356
119 Ls Configuration Options 360
120 rm Parameters 361
121 Web UI Menus 385
122 Switching 411
123 Routing 411
124 NAT Security 412

125 IKE Security 412
126 IPsec Security 412
127 Quality of Service 412
128 Services 413
129 Monitoring 413
130 SIP Session Controller 414
131 MGCP Session Controller 415
132 SIP User Agent 415
133 MGCP User Agent 416

FIGURES

1 BSGX4e Connectivity 30
2 Connect to the Console Port 32
3 Head office and branch office traffic 169
4 Logical path of the routing engine 170
5 VPN operations when NAT is disabled 172
6 VPN operations when NAT is enabled 173
7 Flow types 173
8 Capacity Reduction Between Fast Ethernet and WAN 181
9 GoS Classes 183
10 Strict Policing 184
11 CAR Policing 185
12 Logical path 198
13 Hardware path 199
14 MGCP Network Layout 210
15 Flows that VQM Measures 248
16 VoIP Service Interruption 255
17 SIP Network Layout 264
18 Main Page 379
19 log on Window 381
20 Menu Bar 384

ABOUT THIS GUIDE

This preface describes the intended audience for this guide, how this guide is organized, its conventions, and access to customer support.

Audience

This document provides guidelines for configuring and monitoring the BSGX4e Business Gateway device. It is designed for network managers, administrators, and technicians who are responsible for the management of networking equipment in enterprise and service provider environments. Knowledge of telecommunication technologies and standards, including telephony and Internet protocols, is assumed.

For installation information, see the *BSGX4e Business Gateway Installation Guide* (see "Documentation" (page 26)).

Organization

The following table describes the content and organization of this guide.

Table 1. User Guide Organization

Chapter	Title	Content
		Part I: BSGX4e Use
1	**Connecting to the Device**	Device overview and the means of remote access to the unit.
2	**Initial Setup**	How to set the time, restart timer and Domain Name Service (DNS) server, and a list of initial configuration settings.
3	**User Management**	How to create, modify, remove, and monitor user access to the device.
4	**Command Interface**	How to use commands, including accessing online help, command syntax, showing and saving configurations, and defining autorun commands.
		Part II: Interfaces and Switch Ports
5	**WAN Interface Configuration**	How to configure the Wide Area Network (WAN) interface.
6	**LAN Switch Configuration**	How to configure the Local Area Network (LAN) switch ports and the LAN interface. Topics include Address Resolution Logic (ARL) and layer 2 Quality of Service (QoS).
7	**VLAN Configuration**	How to configure virtual LANs (VLANs).

Table 1. User Guide Organization (continued)

Chapter	Title	Content
8	**Routing Configuration**	How to manage an Address Resolution Protocol (ARP) table, configure static routes, and start the Routing Information Protocol (RIP) daemon.
		Part III: Traffic Protection
9	**Security Configuration**	Security topics, including the firewall, Network Address Translation (NAT), Application Layer Gateway (ALG), and Intrusion Detection System (IDS).
10	**VPN Configuration**	How to configure Virtual Private Networks (VPN) using IP security (IPsec) and Internet Key Exchange (IKE).
11	**GoS Configuration**	How to configure Nortel's layer 3 QoS feature, Guarantee of Service (GoS).
		Part IV: VoIP
12	**SIP Configuration**	How to configure the Source Internet Protocol (SIP) session controller and user agent.
13	**MGCP Configuration**	How to configure the Media Gateway Control Protocol (MGCP) session controller and user agent.
14	**VoIP Configuration**	Voice over Internet Protocol (VoIP) topics common to both SIP and MGCP.
15	**Local Call Routing**	How phone service is maintained by local call routing.
16	**VoIP Services and Relays**	Services available to LAN devices.
		Part V:System Management
17	**Monitoring**	Displays and statistics for monitoring the system.
18	**Monitoring Tools**	Tools including port mirroring and protocol monitoring.
19	**Software Upgrades**	The file system and how to install upgrades of the device software.
		Appendices
A	**Web User Interface**	Introduces the Web User Interface that provides a graphic user interface for the unit.
B	**Third Party Software**	Lists contact information for third-party software applications referenced in this guide.
C	**SSH Functionality**	How Secure Shell (SSH) can secure the remote management of the unit.
D	**TCPdump Expressions**	Lists the primitives that determine which packets are dumped by a *tcpdump* command.

Table 1. User Guide Organization (continued)

Chapter	Title	Content
E	**Standards Compliance**	Lists the data and voice standards to which the device complies.
F	**Rule Compliance**	Describes how the device complies with U.S. Federal Communications Commission (FCC) and Canadian telecommunication rules.
G	**Copyright Information**	Lists copyright acknowledgements and restrictions.

Conventions

The following conventions are used throughout the guide.

Command Prompt Convention

This guide assumes that the Command Line Interface (CLI) is the user's primary method of interaction with the device. When using the CLI, the user enters each command on a command line following the command prompt. The command prompt consists of a string followed by the **>** character. The string can be easily changed, by convention, so this guide shows the command prompt as the greater than **(>)** symbol only.

Text Font Conventions

This guide uses the following text font conventions:

Table 2. Text Conventions

Font	Purpose
NOTE:	*Emphasizes information to improve product use.*
IMPORTANT:	**Indicates important information or instructions that must be followed.**
CAUTION:	**Indicates how to avoid equipment damage or faulty application.**
WARNING:	**Issues warnings to avoid personal injury.**
italic emphasis	Shows book titles, special terms, or emphasis.
bold emphasis	Shows strong emphasis.
`courier font`	Shows a screen capture: what is displayed on the monitor.
`blue screen font`	Emphasizes selected items in a screen capture.
`italic screen font`	Indicates a parameter placeholder in command examples.
`boldface screen font`	Shows commands that you enter or keyboard keys that you press.

Documentation

The documentation for the unit is on the CD-ROM, titled *Nortel BSGX4e Documentation*, that is shipped with the unit. PDF files on the CD contain the following guides:

- *BSGX4e Business Gateway Installation Guide*
- *BSGX4e Business Gateway User Guide*

To view PDF files, use Adobe Acrobat® Reader® 5.0, or later, from your workstation. If Adobe Acrobat Reader is not installed on your system, you can obtain it free from the Adobe website: www.adobe.com

How to get help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- *download software, documentation, and product bulletins*
- *search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues*
- *sign up for automatic notification of new software and documentation for Nortel equipment*
- *open and manage technical support cases*

Getting Help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

1 CONNECTING TO THE DEVICE

This chapter describes the features of the BSGX4e device and its role in an IP network. It also describes how to connect to the device and how to set up remote administrative services.

The BSGX4e is an integrated device, that contains a broad set of networking functionality for voice and data in a single unit:

- It acts as a full-featured router with VoIP, QoS, and advanced security capabilities.
- It slots into the existing network, connected by an Ethernet cable to the WAN access router.
- It enables the effective provisioning of converged VoIP and data services.
- It provides session control and service monitoring of VoIP devices on the LAN, protects against malicious packet attacks, and provides call admission control.
- The BSGX4e includes an Foreign Exchange Station (FXS) port that can provide an analog device with access to VoIP service.
- The BSGX4e includes an Foreign Exchange Office (FXO) port that can provide backup access to the Public Switched Telephone Network (PSTN).

Network Role

Figure 1 shows a possible IP network layout with an BSGX4e unit that connects a LAN to the WAN. The figure illustrates the following:

- The BSGX4e unit can reference servers on the WAN for the devices on its LAN.
- LAN devices can include VoIP phones using SIP or MGCP protocols.
- Through its FXO port, you can connect the BSGX4e device to a CO line (PSTN) that acts as a lifeline if VoIP service is not available.
- The unit can provide a VoIP connection for an analog device (such as a phone or fax machine).
- Use a console to locally configure and monitor the unit.

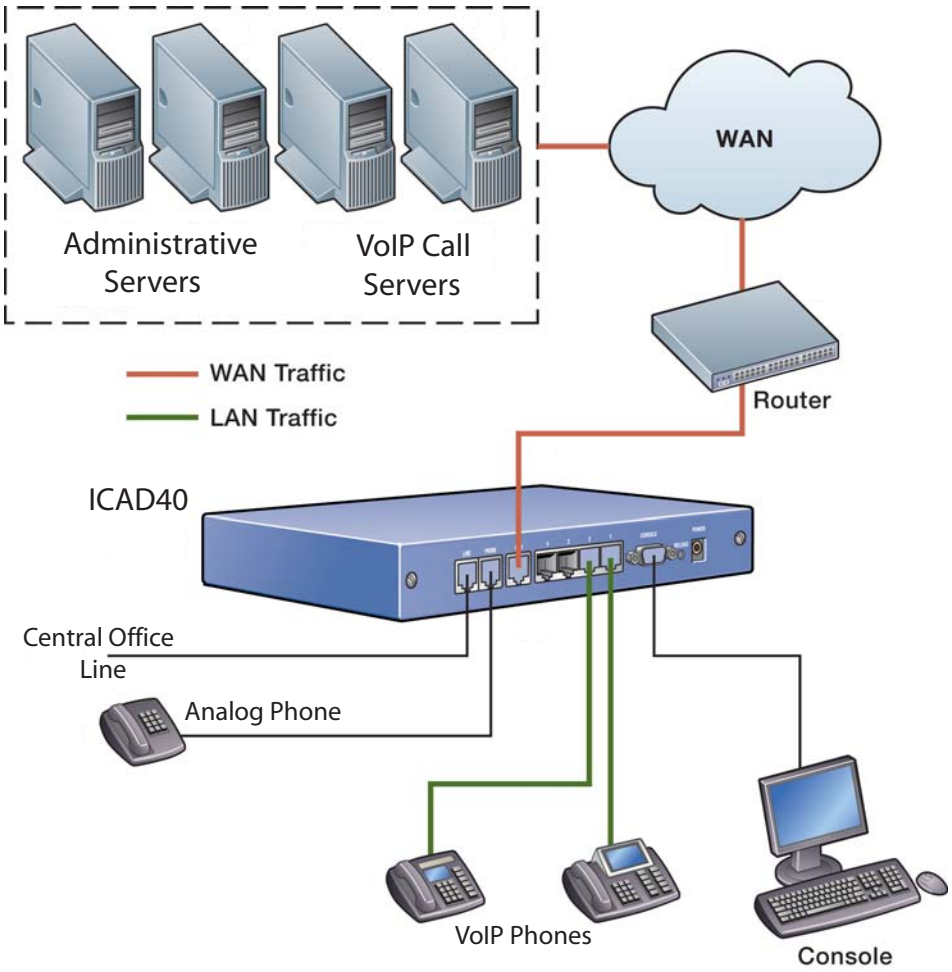


Figure 1. BSGX4e Connectivity

Device Features

An BSGX4e unit provides the following services:

- **VoIP Session Controller**

  The BSGX4e unit acts as the session controller for up to 1000 VoIP phones. It can use the SIP or MGCP protocol and can control up to 500 concurrent calls.

  When the WAN is down, the unit provides VoIP survivability. It can place calls between LAN endpoints and, with its intelligent lifeline, it can switch calls to the PSTN through the emergency backup FXO line.

- **Integrated VoIP Gateway (User Agent)**

  An BSGX4e unit also acts as User Agent (UA) for VoIP phones. It provides a VoIP endpoint within the network, performing signaling, media control, and conversion from traditional interfaces to VoIP.

An BSGX4e unit provides two telephony interfaces: one FXS port for connectivity of analog phones or fax machines and one FXO port to act as a backup lifeline to the PSTN.

- **Security**

  To provide network security, an BSGX4e unit includes a firewall, an advanced Intrusion Detection System (IDS), Application Layer Gateway (ALG), and support for network address translation (NAT) and virtual private networks (VPNs).

- **Multi-Service QoS**

  The BSGX4e unit includes an advanced QoS mechanism called Guarantee of Service (GoS). This easy-to-configure mechanism ensures the optimal priority and bandwidth allocation for multiple classes of critical traffic. It is compatible with DiffServ with support for Terms of Service (ToS) field remarking.

- **LAN Switch**

  An BSGX4e unit includes a 4-port switch, with support for Layer 2 QoS and VLAN segmenting.

- **Monitoring**

  An BSGX4e unit dynamically monitors and provides statistics for both data and voice flows (such as Mean Opinion Score (MOS) scores gathered per call).

- **Management**

  Perform configuration and monitoring by entering commands or by selecting options from a Web browser interface. The management system assures secure remote access with SSH and Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

Connecting to the Unit

This user guide assumes that the BSGX4e unit is installed in a working IP network. The installation procedures are described in the *BSGX4e Business Gateway Installation Guide*.

Configure and monitor this unit by using commands or by using its Web user interface. This user guide describes command use; the Web user interface is introduced in *"Web User Interface" (page 379)*.

The "Remote Administration Services" (page 33) describes the servers that can provide remote access to the BSGX4e unit. Remote access requires the IP address of the unit. If the IP address is unknown, you can determine the IP address during a console session as described in the following section.

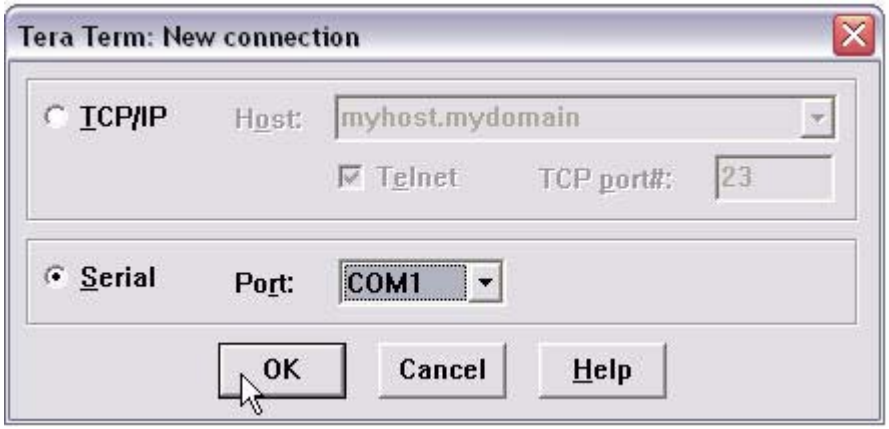
Finding an IP Address using a Console Session

This procedure assumes the following:

- A workstation is connected to the CONSOLE port of the BSGX4e through a serial port cable.
- The workstation is running Tera Term Pro or a similar terminal emulator.

  Note: This procedure uses Tera Term Pro (see "Third Party Software" (page 399)).

1. Connect to the BSGX4e through the terminal emulator:



a Select File, and then, New Connection from the menu bar. A window opens titled *Tera Term: New Connection.*

b Select the Serial button.

c Select the appropriate COM Port.

d Click OK.

Figure 2. Connect to the Console Port

2. Enter a user name, such as nnadmin, after the prompt:

```
User:
```

3. **Enter the password for the user account.**
   Password:
   The initial password is PlsChgMe!; it may have been changed during installation.
4. **System information is displayed, ending with the command prompt that ends with the greater than (>) symbol.**
5. **After the command prompt, enter the following command:**
   > **show interface ip**

   A display similar to the following appears:

```
"eth0" info:

   Interface           eth0
   Flags             (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP MULTICAST
   IP Address/Mask     172.16.1.217/255.255.255.0
   MTU                 1500
   DHCP                off
   Lease obtained      N/A
   Lease expires       N/A
   MAC Address         00:15:93:FF:00:F8
   Speed               FULL100
   Configured speed    AUTONEG

"eth1" info:

   Interface           eth1
   Flags             (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP MULTICAST
   IP Address/Mask     192.168.1.1/255.255.255.0
   MTU                 1500
   DHCP                off
   Lease obtained      N/A
   Lease expires       N/A
   MAC Address         00:15:93:FF:00:F9
   Speed               N/A
   Configured Speed    N/A
```

6. **Find the IP address on the `IP Address/Mask` line for the interface to be used:**

   If connecting to the BSGX4e through the WAN, use the `eth0` address.

   If connecting to the BSGX4e through a LAN port, use the `eth1` address.

Remote Administration Services

This section describes how to configure servers that allow for remote administration of the BSGX4e unit. These servers are:

- Telnet server
- Secure Shell (SSH) server
- Web server
- Secure Socket Layer (SSL) server

The Telnet server in the unit is initially disabled, you must open a connection to the unit from a Telnet session on a workstation. For more information, see *"Telnet Access" (page 34)*.

The SSH server in the unit is also initially enabled. It provides a means of secure, remote access. For more information, see "SSH Server" (page 36).

The Web server is initially enabled to allow the use of the Web user interface. Access to the Web server is described in "Web Server" (page 38).

Show Remote Connections

The maintenance command **whoison** shows the users that are currently using remote access to the unit. An example follows:

```
> whoison

User                Source IP           Type
-------------------------------------------------------------
admin                Unknown             Terminal
user                 10.0.1.2            Web
```

The **Type** field indicates how the user is connected to the unit: Terminal (console port), SSH, Telnet, or Web.

Telnet Access

Telnet allows access to the BSGX4e unit through a remote terminal session. Telnet access requires the following:

- The workstation on the WAN or LAN must provide a Telnet client (for example, Tera Term Pro, Windows telnet client, or Linux telnet client).
- As initially configured, the Telnet server in the unit is enabled, and the firewall allows Telnet access from the WAN.

If the initial unit configuration is changed, the following reconfiguration can be required:

- For Telnet access from the WAN, the firewall must allow Telnet traffic terminating at the BSGX4e device. This requires a security policy for TCP traffic to the Telnet port (The default Telnet port is port 23). For more information about security policies, see "Firewall Security Policies" (page 130).
- The Telnet server on the unit must be configured and enabled as described in the following section "Telnet Configuration Command" (page 34).

Telnet Configuration Command

To change the Telnet configuration, enter the following command:

```
> config service telnet
```

Table 3 describes the parameters for `config service telnet`.

Table 3. Telnet Server Configuration Parameters

Parameter	Description
enabled	Enables the Telnet server (Boolean). Initially, Telnet is enabled.
port	Telnet server port number. The default is **23**.

Telnet Configuration Example

The following example disables the Telnet server on port 23.

```
> config service telnet no enabled
*> save
```

Show Telnet Configuration

To verify the Telnet configuration, enter the following command:

```
> show service telnet

Telnet Service:

   Enabled      no
   Port         23
```

Telnet Client Command

To start a Telnet session, enter the following command:

```
> telnet
```

Table 4 describes the parameters for the maintenance command `telnet`.

Table 4. Telnet Parameters

Parameter	Description
ip address	IP address of the BSGX4e device.
-p	Optional Telnet port number.

Telnet Session Example

The following example starts a Telnet session on the device at IP address 192.168.134.217:

```
> telnet 192.168.134.217

Trying 192.168.134.217
Connected to 192.168.134.217
Escape character is '^]'.
User:
```

SSH Server

This section describes how to configure the Secure Shell (SSH) server. The SSH server enables secure remote access to the BSGX4e device over an insecure network, such as the Internet. SSH version 2 is supported.

SSH use requires the following:

- The workstation on the WAN or LAN must provide an SSH client (for example, PuTTY or SSH secure shell).
- As initially configured, the SSH server in the unit is enabled, and the firewall allows SSH access from the WAN.

If the initial unit configuration is changed, the following reconfiguration can be required:

- For SSH access from the WAN, the firewall must allow SSH traffic terminating at the BSGX4e device. This requires a security policy for TCP traffic to the SSH port. (The default SSH port is port 22). For more information about security policies, see "Firewall Security Policies" (page 130).
- The SSH server on the unit must be configured and enabled as described in the section "SSH Configuration Command" (page 36).

Digital Signature Algorithm (DSA) Host Keys

The SSH server uses a set of 640-bit DSA host keys (one public, one private) for data encryption. It stores one set of keys on the file system (`/cf0sys/ssh`). A randomly seeded algorithm generates an initial set of host keys the first time that the BSGX4e device is started. The SSH server uses this set of host keys to identify itself when an SSH client connects. Regenerate new host keys by using the parameter `hostkeys` on the **config service ssh** command.

After a secure connection is established between the SSH server and a client, the client attempts authentication. The SSH server supports password, keyboard, and publickey authentication.

- When both `password` and `keyboard` authentication are requested, the user must supply a username and password.
- To use `publickey` authentication, upload files containing the public key of the SSH client must be to the device in the directory:
  `/cf0sys/id_<username>.pub.`

After the SSH client is authenticated, it requests an SSH secure remote log on.

SSH Configuration Command

To change the SSH configuration, enter the following command:

```
> config service ssh
```

Table 5 describes the parameters for `config service ssh.`

Table 5. SSH Configuration Parameters

Parameter	Description
enabled	Enables the SSH server (Boolean). The initial setting is enabled.
port	SSH server port number. The default is **22**.
hostkeys	Host keys that the SSH server uses to authenticate itself (**none** | **640bit**). The default is **640bit**. To regenerate the SSH keys, set `HostKeys` to `none`, and then to `640bit`.
authmethods	Permitted authentication methods (**all** | **keyboard | password | publickey** | **none**). The default is **all**.
services	Permitted SSH services (**all** | **ssh | sftp** | **none**). The default is **all**.

SSH Example

The following example disables SSH service.

```
> config service ssh no enabled
*> save
```

Show SSH Configuration

To verify the configuration, enter the following command:

```
> show service ssh

SSH Service:

   Enabled          yes
   Port             22
   HostKeys         640bit
   AuthMethods      keyboard + password + publickey
   Services         ssh + sftp
```

Regenerate SSH keys

To regenerate the SSH keys, set the parameter `HostKeys` to `none`, and then to `640bit`. An example follows:

```
> config service ssh hostkeys none
*> config service ssh hostkeys 640bit
*> show service ssh

SSH Service:

   Enabled          yes
   Port             22
```

```
HostKeys        generating...
AuthMethods     keyboard + password + publickey
Services        ssh + sftp
```

The key regeneration can take several seconds. During this period, the value of the parameter HostKeys is generating....

Upload Public Key

To upload the public key of an SSH client, use a Simple File Transfer Protocol (SFTP) session.

The following example uploads the key of client *fred* to the BSGX4e device, IP address 192.168.134.217.

1. **Start the SFTP session:**

```
fred@cygnus ~ $ sftp admin@192.168.134.217

Connecting to 192.168.134.217...
The authenticity of host '192.168.134.217 (192.168.134.217)'
can't be established.
DSA key fingerprint is
9a:1f:34:52:f1:78:d7:6c:56:5b:9d:73:f0:da:1f:c0.

Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.134.217' (DSA) to the
list of known hosts.

User: nnadmin
Password:
sftp> cd /cf0sys
sftp> put id_fred.pub

Uploading id_fred.pub to /cf0sys/id_fred.pub
```

2. **To view the contents of the directory, enter the following command:**

```
sftp> ls

flash         id_fred.pub   ssh           ssl
```

Web Server

This section describes how to configure the Web server. The Web server enables the remote administration of the BSGX4e device using the Web User Interface (see “Web User Interface” (page 379)).

The Web server supports access through Hypertext Transfer Protocol (HTTP) and HTTPS (HTTP over SSL). For more information on SSL configuration, see “SSL” (page 40).

Web server use requires the following:

- The workstation on the WAN or LAN must provide a Web browser (Microsoft Internet Explorer or Mozilla Firefox).
- As initially configured, the Web server in the unit is enabled, and the firewall allows HTTP or HTTPS traffic from the WAN terminating at the BSGX4e.

NOTE: The initial unit configuration enables the Web server and configures a security policy to allow Web access from the WAN to the unit.

If the initial unit configuration is changed, the following reconfiguration can be required:

- For Web access from the WAN to the unit, the firewall must allow Web traffic terminating at the BSGX4e device. This requires access for TCP traffic to the Web and Web User Interface (UI) ports. (The default Web UI port is port 443; the default Web port is 80.) For more information about the firewall, see "Firewall Security Policies" (page 130).
- Configure and enable the Web server in the unit as described in the following section "Web Server Configuration Command" (page 39).

Web Server Configuration Command

To change the Web server configuration, enter the following command:

```
> config service web
```

Table 6 describes the parameters for `config service web`.

Table 6. Web Server Configuration Parameters

Parameter	Description
enabled	Enables the Web server (Boolean). Initially, the Web server is enabled.
httpport	HTTP port number for the Web server. The default is **80**.
httpsport	HTTPS port address for the Web server. The default is **443**.

Disable Web Server Example

The following example disables the Web server.

```
> config service web no enabled
*> save
```

Show Web Server Configuration

To verify the configuration, enter the following command:

```
> show service web

Web Server:

   Enabled        yes
```

```
HTTP Port       80
HTTPS Port      443
```

Show Web Server Statistics

To display the statistics of the Web server, enter the following command:

```
> stats service web

Web Stats:

Redirects       0                               Errors          0
Access Err      0                               Timeouts        0
Form Hits       0                               Local Hits      0
```

Table 7 describes the Web server statistics.

Table 7. Web Server Statistics

Statistic	Description
Redirects	Number of redirections from the Web server.
Errors	Number of Web server errors.
AccessErr	Number of security violations from the Web server.
Timeouts	Number of timeouts from the Web server.
FormHits	Number of form requests.
LocalHits	Number of local hits for access.

SSL

This section describes how to configure the Secure Socket Layer (SSL). SSL enables secure remote access to the BSGX4e device over an insecure network, such as the Internet.

The steps required to configure SSL are:

1. **Generate a new SSL key if the existing key has been deleted or compromised.**
2. **Generate a new SSL certificate signing request (CSR).**
3. **Generate or import the SSL certificate.**

SSL Key

The system administrator can use the SSL key to manage a private Rivest Shamir Adleman (RSA) key, which the SSL server requires to encrypt data. The first time the BSGX4e device is started, a randomly-seeded, 1024-bit RSA key is generated and saved. Normally, a new private key does not need to be generated unless the security of the private key has been compromised. The RSA key is stored in the file `/cf0sys/ssl/rsakey.dat`.

NOTE: If the SSL key is deleted, new SSL connections cannot be created. To see the status of the SSL key, enter **show ssl key.**

A new SSL key can be generated. The number of bits is constrained to 512, 768, 1024, or 2048. When the SSL key record is created or modified, a key generation task is started. Key generation can take several minutes, depending on the size of the key. When key generation starts, the key used by the SSL server is deleted; new SSL connections cannot be created until a new key is available. When key generation completes, the RSA key used by the SSL server is set to the newly generated key; new SSL connections can then be created.

SSL Key Command

To generate a new SSL key, enter the following command:

```
> config ssl key
```

Table 8 describes the parameters for `config ssl key`.

Table 8. SSL Key Configuration Parameters

Parameter	Description
[type]	Type of encryption key (**RSA**).
bits	Number of bits in key (**512** | **768** | **1024** | **2048**).

SSL CSR

A system administrator can use the SSL Certificate Signing Request (CSR) to generate an X509 certificate, which can be self-signed by the SSL module or signed by an external certificate authority (CA).

A single X509 CSR can be generated. Generating a CSR requires an SSL key. To see the status of the SSL key, enter **show ssl key**.

NOTE: If the SSL CSR is deleted, new SSL connections cannot be created.

SSL CSR Command

To generate an SSL CSR, enter the following command:

```
> config ssl csr
```

Table 9 describes the parameters for `config ssl csr`.

Table 9. SSL CSR Configuration Parameters

Parameter	Description
[type]	Certificate signing request type (**x509**).
country	Two-letter country code. The default is US for the United States; to see the most recent list, go to www.iso.org
state	Full name of state or province (such as, California).

Table 9. SSL CSR Configuration Parameters (continued)

Parameter	Description
locality	Locality or city name (such as, Fremont).
orgname	Company name (such as, NewCo).
orgunit	Organizational unit (such as, Engineering).
commonname	Domain name (such as, www.example.com).
email	E-mail address (such as, webadmin@example.com).

Upload SSL CSR

Use SFTP to upload an SSL CSR. The recommended directory for the uploaded CSR file is **/cf0sys/ssl**. An example follows.

1. Upload the SSL CSR file:

```
fred@cygnus ~ $ sftp admin@192.168.134.217

Connecting to 192.168.134.217...
The authenticity of host '192.168.134.217 (192.168.134.217)'
can't be established.
DSA key fingerprint is
9a:1f:34:52:f1:78:d7:6c:56:5b:9d:73:f0:da:1f:c0.

Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.134.217' (DSA) to the
list of known hosts.
User: nnadmin
Password:
```

2. Set the current directory and store the CSR file in it:

```
sftp> cd /cf0sys/ssl
sftp> put csr.pem
Uploading csr.pem to /cf0sys/ssl/csr.pem
```

3. Ensure that the CSR file is in the current directory:

```
sftp> ls
rsakey.dat          csr.pem
```

At this point, use the imported CSR to generate the SSL certificate as described in the next section "SSL Certificate" (page 42).

```
> config ssl certificate x509 import /cf0sys/ssl/csr.pem
*> save
```

SSL Certificate

A system administrator can use the SSL certificate to configure an X509 certificate used by the SSL server. Two methods exist to configure the X509 certificate: either the SSL CSR record is self-signed, or the SSL CSR is signed by an external certificate authority and an X509 certificate is imported into the SSL certificate.

A single X509 certificate can be generated. When self-signed, the certificate is derived from the current CSR record and key record.

NOTE: **A self-signed certificate can be generated only if an SSL key record and an SSL CSR record exist.**

Alternately, you can import an SSL certificate using a file containing a certificate signed by an external certificate authority (CA). The certificate must be in Privacy Enhanced Mail (PEM) format with no header before the "----- BEGIN CERTIFICATE -----" text. When a CA-signed certificate is imported, the certificate is checked to ensure that it is in the correct PEM format. If the format is incorrect, the certificate is not imported.

NOTE: If the SSL certificate is deleted, new SSL connections cannot be created.

SSL Certificate Command

To generate the SSL certificate, enter the following command:

```
> config ssl certificate
```

Table 10 describes the parameters for `config ssl certificate`.

Table 10. SSL Certificate Configuration Parameters

Parameter	Description
[type]	Certificate type (**x509**).
signed	Self-signs the current CSR (**self** | **null**).
import	PEM format file from which to import the certificate.

SSL Configuration Example

This example generates an RSA key of 768 bits. It then generates an SSL CSR for the Sells unit of the company EiffelGroup in Paris, France. Finally it generates a self-signed SSL certificate.

```
> config ssl key rsa bits 768
*> config ssl csr x509 country FR no state locality Paris
orgname EiffelGroup orgunit Sells commonname
www.eiffelgroup.com email contact@eiffelgroup.com
*> config ssl certificate x509 signed self
*> save
```

Show SSL Configuration

To verify the SSL configuration, enter the following commands:

```
> show ssl key
SSL Key:

Type       rsa
```

```
Bits        768
Status      ok
```

(While key generation occurs, the Status field displays generating…. After key generation is complete, it displays ok.)

```
> show ssl csr

SSL Certificate Signing Request:

Type            x509
Country         FR
State
Locality        Paris
OrgName         EiffelGroup
OrgUnit         Sells
CommonName      www.eiffelgroup.com
Email           contact@eiffelgroup.com
Status          ok
PEMData         -----BEGIN CERTIFICATE REQUEST-----
MIIBkDCCARkCAQAwgZQxCzAJBgNVBAYTAkZSMQkwBwYDVQQIEwAxDjAMBgNVBAcTB
VBhcmlzMRQwEgYDVQQKEwtFaWZmZWxHcm91cDEOMAwGA1UECxMFU2VsbHMxHDAaBg
NVBAMTE3d3dy5laWZmZWxncm91cC5jb20xJjAkBgkqhkiG9w0BCQEWF2NvbnRhY3R
AZWlmZmVsZ3JvdXAuY29tMHswDQYJKoZIhvcNAQEBBQADagAwZwJgQKmzUXzjbaLl
QXybKsRNTp7+MmMR2vBODvLCqRgLi78AdXkZV2Yy0xfWqTGPRJ1sVOdQmXoWA2nus
va+SEClTuoL92Qnx9qI7NbjrWLn02ZHTflaOBdb2npMgIwbjJ3LAgMBAAGgADANBg
kqhkiG9w0BAQQFAAOBYQAnzBtWdcRLKcX8CObgdkM4jcdhm07giSiBT/wcEQNNk5A
WBlMnubSd2pHzADm3eM2tADQZTs88SnkXm/vdaDrGilxOu44I05xBsgPVnPn/0eo9
i/JxqrulQxgeoVADTds=
-----END CERTIFICATE REQUEST----
```

The Status field shows the status of the CSR, as follows:

no key	There is no SSL key.
waiting for key generator…	The certificate request is being generated.
ok	Generation is complete; an SSL key is available, and the PEMData field shows the actual CSR in the standard PEM format.

```
> show ssl certificate

SSL Certificate:

Type                x509
Country             FR
State
Locality            Paris
OrgName             EiffelGroup
OrgUnit             Sells
CommonName          www.eiffelgroup.com
Sha1FingerPrint     69 1F 98 DC BC 11 6D AB 06 5C BF 81 A6 C6
82 EF 7A D6 3A BC
```

```
Status                ok
```

The `Sha1FingerPrint` field displays the Secure Hash Algorithm-One (SHA1) fingerprint of the certificate.

The `Status` field indicates the status of a self-signed certificate:

`no key`	No SSL key record exists; generate a new key.
`no csr`	No SSL CSR exists; generate a new CSR key.
`waiting for key generator…`	The certificate is being generated.
`ok`	Certificate generation is complete.

2 INITIAL SETUP

This chapter describes the initial setup of the BSGX4e device, including:

- system time and SNTP server configuration
- watchdog reset timer
- DNS server configuration
- default configuration settings

For information about customizing the command line, see "Customizing the Command Session" (page 78).

Setting the Time

Two methods exist for setting the system time for the BSGX4e unit.

- Acquire the time from the IP network through the SNTP protocol. Specify up to four SNTP servers.
- Set the local time manually.

NOTE: If DHCP is enabled and a DHCP server is available, the DHCP server can provide SNTP server information to the BSGX4e. To see the current SNTP configuration, enter **show system sntp**.

Show the Current Time

To display the current time, enter the following command:

```
> time
FRI NOV 10 8:10:02 2006
```

Setting the Time Manually

To set the time for the unit, enter the **time** command specifying the desired time and date values, as follows:

- Specify the time as: **-t** *hh:mm:ss*
- Specify the date as: **-d** *dd:mm:yyyy*

Time Setting Example

To set the time to 2:05 PM on 10 November 2006,enter the following command:

```
> time -t 14:05:00 -d 10:11:2006
```

NOTE: The time is changed immediately; you do not need to enter **save**.

Setting the Time through an SNTP Server

The unit can automatically synchronize its internal time to the time provided by an SNTP server. For automatic time synchronization:

- The SNTP client configuration must specify at least one SNTP server and the appropriate time zone offset.
- The SNTP client must be enabled.

NOTE: To change an SNTP server, the SNTP client must be disabled.

SNTP Configuration Command

To configure the SNTP service, enter the following command:

```
> config system sntp
```

Table 11 describes the parameters for `config system sntp`.

Table 11. SNTP Server Configuration Parameters

Parameter	Description
enabled	Enables the SNTP client (Boolean) To enable, specify **enabled**. To disable, specify **no enabled**. The client is initially disabled.
server1	IP address or Fully Qualified Domain Name (FQDN) of an SNTP server.
server2	IP address or FQDN of an SNTP server.
server3	IP address or FQDN of an SNTP server.
server4	IP address or FQDN of an SNTP server.
gmtoffset	Time zone offset from Greenwich Mean Time (GMT) ([**+**|**-**]*hh*:*mm*, hours and minutes, positive or negative).
sync	Interval for resynchronization of the internal clock to the network time (external clock) (in days,**1**—**31**). The default value is **seven**.

SNTP Client Example

This example enables the SNTP client and specifies the name of the SNTP server and the time zone offset.

FQDN of SNTP server : `ntpserver.wan.com`
GMT offset: one hour forward (+1)

```
> config system sntp enabled server1 ntpserver.wan.com
gmtoffset +1
*> save
```

Show SNTP Configuration

To see the SNTP client configuration, enter the following command:

```
> show system sntp
```

```
SNTP:
   Enabled           on
   Server 1          ntpserver.wan.com
   Server 2          0.0.0.0
   Server 3          0.0.0.0
   Server 4          0.0.0.0
   Gmt Offset        +01:00
   Sync Interval     7 days
   Last Sync         FRI FEB 17 15:53:25 2006
   Next Sync         FRI FEB 24 15:53:25 2006
```

Changing SNTP Servers

To change the SNTP servers, disable the SNTP client first. The following command sequence clears the second SNTP server:

```
> config system sntp no enabled
*> config system sntp no server2
*> config system sntp enabled
*> save
```

Watchdog Reset Timer

The watchdog reset timer allows the BSGX4e unit to automatically restart after a software failure. This timer is required because such a failure could possibly "freeze" the unit so that no traffic can be routed through it. The automatic reset allows the unit to recover from that state and restores it to normal operation.

NOTE: It is recommended that the initial watchdog configuration remain unchanged. The initial configuration enables the reset timer and sets its value to seven seconds.

Watchdog Timer Command

To configure the watchdog timer, enter the following command:

```
> config system watchdog
```

Table 12 describes the parameters for `config system watchdog`.

Table 12. System Watchdog Configuration Parameters

Parameter	Description
enabled	Enables the watchdog timer (Boolean). Initially, the timer is enabled.
refresh	Refresh interval for the timer (in seconds). The default is **seven** seconds.

Watchdog Timer Example

The following example enables the watchdog and sets its refresh interval to five seconds.

```
> config system watchdog enabled refresh 5
*> save
```

Show Watchdog Configuration

To show the current watchdog configuration, enter the following command:

```
> show system watchdog

Watchdog Configuration:
Watchdog Enabled     yes
Refresh interval     5 seconds
```

DNS Client

The Domain Name Service (DNS) client in the unit sends requests to a DNS server on the WAN. The DNS requests get IP addresses required by the BSGX4e, such as the IP address of a SIP server specified by FQDN. Two DNS servers can be configured: one primary, the other as a secondary, backup server.

The DNS client determines the DNS configuration to use based on the current value of its **source** parameter:

- **User**: The DNS client uses the latest DNS configuration provided by the user.
- **DHCP**: The DNS client uses the DNS configuration provided by the DHCP server.
- **PPP**: The DNS client uses the DNS configuration provided by the PPP server.

NOTE: The command **show system dns** *shows the DNS configuration currently in use.*

DNS Client Configuration Command

To configure the DNS client, enter the following command:

```
> config system dns
```

This command can:

- Specify the source of the DNS configuration the client is to use (DHCP, or user). The default is DHCP.
- Specify a user-provided DNS configuration. This configuration is always stored, but it is used only when the **source** parameter value is set to user.
- Specify an optional domain name that is appended to every DNS request.

Table 13 describes the parameters of `config system dns`.

Table 13. DNS Client Configuration Parameters

Parameter	Description
dns1	IP address of the primary DNS server.
dns2	IP address of an optional, secondary DNS server.
domain	Domain name for the unit. For a name that is not an FQDN, the DNS client adds the domain to the host before querying the DNS server. Example: If the specified name is host and the specified domain is domain.com, the query is for host.domain.com.
source	Source of the DNS configuration (user | dhcp | ppp). The default is dhcp. **user** Use the latest user-provided configuration. **dhcp** Use the configuration provided by the DHCP server. If DHCP is disabled, **dns1** is set to 0.0.0.0 and **dns2** and **domain** are cleared. **ppp** Use the configuration provided by the PPP server. If no PPP interface is active, dns1 is set to 0.0.0.0 and **dns2** and **domain** are cleared.

DNS Client Configuration Example

This example shows how the configuration used by the DNS client can change.

1. Assume that DHCP is running and the DNS client uses the default DNS server configuration provided by the DHCP server.

```
> show system dns

DNS Settings:

   DNS1    172.29.0.1
   DNS2    0.0.0.0
   Domain  wan.com
   Source  dhcp
```

2. Enter a fixed, user-provided DNS server configuration. The **source** parameter is not changed to **user** so the new, user-provided configuration is stored, but not used.

```
> config system dns dns1 192.168.1.2
> show system dns

DNS Settings:

   DNS1    172.29.0.1
   DNS2    0.0.0.0
   Domain  wan.com
   Source  dhcp
```

3. Change the source parameter to user and the previously entered, user-provided configuration is used.

```
> config system dns source user
> show system dns

DNS Settings:

   DNS1    192.168.1.2
   DNS2    0.0.0.0
   Domain
   Source  user
```

Show DNS Client Configuration

To see the configuration currently in use by the DNS client, enter the following command:

```
> show system dns

DNS Settings:

   DNS1    192.168.134.160
   DNS2    0.0.0.0
   Domain  wan.com
   Source  dhcp
```

Check DNS Server Accessibility

After the configuration is complete, ensure that the DNS server is accessible. To do this, `ping` a device by name. The ping command references the DNS server to translate the name to an IP address.

In the following example, assume that the domain is configured as wan.com. The example pings a SIP server on the LAN named `sipserver`.

```
> ping sipserver
Pinging sipserver.wan.com (192.168.134.162): 56 data bytes

Reply from 192.168.134.162: bytes=56 icmp_seq=0 time<1ms
Reply from 192.168.134.162: bytes=56 icmp_seq=1 time<1ms
Reply from 192.168.134.162: bytes=56 icmp_seq=2 time=5ms
Reply from 192.168.134.162: bytes=56 icmp_seq=3 time<1ms

----- sipserver.wan.com ping statistics -----
4 packets transmitted, 4 packets received, 0.0% packet loss
Round-trip times: min/avg/max=0/0/5ms
```

Initial Settings

To list the current configuration of the unit, enter a **dump** command.

Table 14 lists the initial settings of the unit when it is shipped. It also references the sections in this guide where the settings are discussed.

Table 14. Initial Settings

IP Interface	Initial Settings	To change, go to:
eth0	IP address: 0.0.0.0 No IP mask DHCP client is on (enabled)	"eth0 Configuration Command" (page 92)
eth1	IP address/mask: 192.168.1.1/255.255.255.0 DHCP client is off (disabled)	"LAN Interface (eth1)" (page 102)
User Groups		*"User Groups" (page 64)*
admins	access: ssh + Web + cli + telnet + ftp All access permissions	
users	access: Web + cli	
User Accounts		*"User Accounts" (page 61)*
admin	access ssh + Web + cli + telnet + ftp group1 admins group2 users group3 admins group4 admins group5 admins password admin	
user	access Web + cli group2 users group3 users group4 users group5 users password netcat	
User Rights		*"User Rights" (page 66)*
admin	access read and write all objects, including configuration commands gname admins object Admins	
useradv	access read gname users object Admins	
userbasic	access read + write gname users object Users	

Table 14. Initial Settings (continued)

Security Policies	Traffic from WAN to LAN is rejected. Traffic from WAN terminating at the unit is rejected, except for Web UI, SSH, and Telnet traffic.	*"Firewall Security Policies" (page 130)*
SSH access from WAN to unit allowed	Seq 1 From eth0 To self Destination Port 22 Protocol tcp	
Web UI (HTTPS) access from WAN to unit allowed	Seq 3 From eth0 To self Destination Port 443 Protocol tcp	
Web (HTTP) traffic from WAN to unit allowed	Seq 5 From eth0 To self Destination Port 80 Protocol tcp	
Telnet access from WAN to unit allowed	Seq 7 From eth0 To self Destination Port 23 Protocol tcp	
Voice Settings	jitter buffer type: ADAPTIVE threshold: 0 gain: Tx -3 Rx -3 Telephony port is set for U.S.A. telephones.	*"FXS Port Configuration" (page 238)*
Media Settings	Real-time Transport Protocol (RTP) 13000 - 14999 Default range for source User Datagram Protocol (UDP) port values of RTP traffic is bridged by the unit. LAN to LAN communications are bridged through the unit. 500 calls are allowed.	*"Media Bridge (MBR)" (page 229)*
Voice ACL Policies	All LAN SIP or MGCP endpoints are allowed to originate and receive calls. Seq 1 Stats 0	*"Access Control List (ACL)" (page 232)*
Layer 2 QoS	Disabled.	*"Layer 2 QoS" (page 106)*
Telnet server	Enabled.	*"Telnet Access" (page 34)*

Table 14. Initial Settings (continued)

SSH server	Enabled. AuthMethods: keyboard + password + publickey Services: ssh + sftp	*"SSH Server" (page 36)*
Web server	Enabled.	*"Web Server" (page 38)*
Logging	Audit logging: enabled (**show audit log**) Remote module logging (udplog and syslog): disabled. Local module logging: enabled (**show logging internal**)	*"Audit Logging" (page 324)* and "Module Logging" (page 325).
Watchdog reset timer	Enabled.	"Watchdog Reset Timer" (page 49)
SNTP client	Enabled because of DHCP.	"Setting the Time through an SNTP Server" (page 48)
DNS client	Enabled because of DHCP.	"DNS Client" (page 50)
SNMP	Enabled.	"SNMP Agent" (page 347)
NAT	Enabled on the WAN interface (eth0).	"Configuring NAT" (page 134)
ALG	Enabled.	"ALG Configuration" (page 140)
IDS	Enabled.	"IDS" (page 140)
DHCP server	Enabled. Configured on the eth1 interface, when a LAN device requests an IP address, the server can assign an address from its address pool 192.168.1.50-192.168.1.250/24.	"DHCP Server" (page 309)
DHCP relay	Disabled.	"DHCP Relay" (page 312)
DNS relay	Disabled.	"DNS Relay" (page 313)
TFTP relay	Disabled.	"TFTP Relay" (page 316)
SNTP relay	Disabled.	"SNTP Relay" (page 315)
SIP session controller	Disabled.	"SIP Session Controller" (page 271)
SIP gateway	Disabled.	"SIP Gateway" (page 278)
MGCP session controller	Disabled.	"MGCP Session Controller Configuration" (page 215)
MGCP gateway	Disabled.	"MGCP Gateway" (page 222)
GoS traffic protection	Disabled.	"GoS Configuration" (page 181)
RIP daemon	Disabled.	"Starting the RIP Daemon" (page 126)

Table 14. Initial Settings (continued)

VLAN	Disabled.	"VLAN Configuration" (page 111)
Netflow agent	Disabled.	"Netflow Exporter" (page 343)
PMON agent	Disabled.	"Protocol Monitoring (PMON)" (page 340)

3
USER MANAGEMENT

This chapter describes how to control access to the BSGX4e unit:

- password entry
- adding and removing users
- setting up groups
- assigning permission to users and to groups
- authentication using a Radius server or a TACACS+ server

IMPORTANT: The security of the BSGX4e unit depends on password security. To ensure secure access to the unit, change passwords regularly and keep them secure.

NOTE: To perform user management functions that change the user management database, you must log on with a user ID that has both read and write access. The pre-defined user ID **nnadmin** *has all access rights.*

User Management Features

The user management functions determine who can access the BSGX4e unit and whether the user can change the configuration of the unit or just display information stored in it.

User access is controlled both at logon and after log on:

- At log on, user access is determined by the user ID and password:
  - The user ID determines if the access method is allowed (for example, remote access can be denied to the user).
  - The password must be authenticated (either internally or externally) before access is allowed.
- After log on, the user's access rights limit what the user can do.

You can perform user management functions through a console directly connected to the unit or remotely by using Telnet or SSH. In both cases, you must log on with a valid user account. You can also perform user management functions by using the Command Line Interface (CLI) or the Web user interface (Web UI). For information about using Web UI, see *"Web User Interface" (page 379)*.

The following is a summary of user management functions:

- **Requires log on with a valid user ID and password:**

- Authenticates the entered password by using either strong password hashing (SHA) or external authentication through a Radius server.
- Never stores passwords in clear text.

- **Tracks log on attempts:**
  - Locks out the console port after three failed log on attempts.
  - Keeps a log of all failed log on attempts and logouts.
- **Can limit user accounts to specific access methods, including CLI, Web UI, Telnet, SSH, and/or File Transfer Protocol (FTP).**
- **Lists who is currently logged in to the system:**
  - User list includes their access methods and their IP addresses, if any.
  - Multiple users can log on simultaneously.
- **Supports management of users by user groups:**
  - Users can belong to more than one group.
  - Each user management element (user accounts, user groups, and associated rights records) can be added, edited, and deleted independently.
  - Can assign rights to read and/or write access by user account and by user group.
  - Enforces who has access to which modules in the system, using specified access methods and under what conditions.
- **Provides an audit log that records:**
  - Account activities.
  - Logins and logouts.
  - All failed log on attempts.

Password Entry

All access to the BSGX4e unit requires the entry of a valid user ID and password. The factory settings for the unit define two user IDs:

- **nnadmin** with initial password **PlsChgMe!**
- **user** with initial password **netcat**

The installation procedure recommends that these passwords be changed immediately.

NOTE: For security reasons, it is recommended that all passwords be changed on a regular basis.

Failed log on Attempts

A user can attempt to log on from the console port three times. If the user log on fails all three times, the console is locked out, and no one can log on to the console port for the next fifteen minutes or until the unit is restarted by a power recycle.

When attempting to log on remotely through Telnet or SSH, the user is given three log on attempts, and then the session is ended.

All invalid log on attempts are recorded in the audit log. For more information about the audit log, see “Audit Logging” (page 324).

Changing a Password

Changing a password depends on whether the user account uses internal or external authentication (as determined by its auth parameter; see “User Accounts” (page 61)) If a user account uses internal authentication, the password for the account can be changed while logged on to the account.

NOTE: If a user account uses external authentication, the external authentication server controls the password for the account. Although the user, while logged on, can change the password stored for the user account, this password is not used for authentication and so the effective password is not changed.

NOTE: The administrator (that is, the user logged in with user ID **nnadmin***) can change the password used for internal authentication for any user account. This is done using the* **config user account** *command described on page 61.*

While logged on, all users can change their own passwords. To change your password, use this procedure:

To change the password while logged on, use this procedure:

1. Enter the command **password**:

   ```
   > password
   ```

2. **Enter the old password:**

   ```
   Old Password: ******
   ```

3. **Enter the new password:**

   ```
   New Password: **********
   ```

4. **Reenter the new password:**

   ```
   Verify Password: **********
   ```

   If the new password is reentered correctly, the unit responds with the following message and the user ID (in this case, `nnadmin`**):**

   ```
   Changed password for 'nnadmin'
   ```

5. **To save the password change, enter:**

   ```
   *> save
   ```

Showing Active Users

To see which users are currently logged in to the unit, use the maintenance command **whoison**; its display shows the source IP address of the user and the type of access in effect. An example follows:

```
> whoison

User                Source IP           Type
-------------------------------------------------------------
admin                Unknown             Terminal
user                 10.0.1.2            Web
```

The **Type** field indicates how the user is connected to the unit: Terminal (console port), SSH, Telnet, or Web.

User Accounts, Groups and Rights

User access to an BSGX4e unit is managed by using user accounts, user groups, and user rights settings. The initial factory settings for the unit define the following:

- **Two user groups**—one for administrators (**admins**) and one for other users (**users**). The **admins** user group is granted all access modes, and the other user group is granted only Web and CLI access.
- **Two user accounts**—one for administrators (**admin**) and one for other users (**user**). The **admin** user is granted all access modes and all access rights; the other user account is granted only Web and CLI access, and its access rights are restricted. The **admin** account belongs to both predefined user groups (**admins** and **users**); the other user account belongs only to the **users** user group.
- **Three rights settings**—one for the **admins** user group and the other two for the **users** user group. All rights are granted to **admins**; the two rights settings for the **users** user group grant read-only access to some objects and read and write access to other objects.

*NOTE: You cannot delete or rename the predefined user management configuration. You cannot delete or rename the two user groups (***admins** *and* **users***), the two user accounts (***admin** *and* **user***), or the three user rights settings (***admin***,** **useradv***, and* **userbasic***).*

User Configuration Commands

Table 15 lists the three user configuration commands.

Table 15. Config User Commands

Command	Configures:
config user account	A user account.
config user groups	A user group.
config user rights	A rights record (grants to a group read and/or write access to certain objects).

User Accounts

Before you add a new user account or change an existing user account, display the current user accounts and user groups by entering the following commands:

```
> show user accounts
> show user groups
```

Then, to add or change an account, use the following command:

```
> config user account
```

NOTE: The maximum number of user accounts that you can define for the BSGX4e unit is 20.

Table 16 describes the parameters for `config user account`.

Table 16. User Account Configuration Parameters

Parameter	Description
[name]	Name of the existing account to be changed or the new account to be added. This parameter is required. If an existing account is specified, only the specified parameter values are changed; all other existing values remain unchanged.
access	Access methods allowed to this user. The default is **none**. **all** All access methods allowed. **none** No access allowed. You can specify that two or more of the following methods are to be connected by using plus (**+**) symbols. **ssh** Secure Shell (SSH) access allowed. **Web** Web User Interface (Web UI) access allowed. **cli** Command Line Interface (CLI) access allowed. **telnet** Remote access through a Telnet session allowed. **ftp** File Transfer Protocol (FTP) access allowed.
auth	Internal or external password authentication. The default is internal Strong Password Hashing (**SHA**). To require external authentication, specify **RADIUS** or **TACACS** and configure an authentication record for this user account. Fore more information , see *"Radius Authentication" (page 68)*.
group1	Required first group to which the user belongs. A user must belong to at least one group and can belong to up to five user groups. The predefined user groups are **admins** and **users**. If another user group is configured, you can assign the user account to that group. To remove the user from a group, specify the group parameter with the value **none**.
group2 **group3** **group4** **group5**	Optional additional user groups to which the user account is assigned.
password	The password assigned to the user. This parameter is required. The password for the user account. Entry of this parameter is required at logon if internal authentication is used. (If external authentication is used, the password entered at logon must be the one defined by the external server.)
inherit	Whether the user account inherits access rights from the groups to which it belongs. The default is **yes**.
enabled	Whether the user account is enabled. The default value is **yes**.

Add User Account Example

This example assumes that the user is given read and write access to the unit, but only while connected directly to its console port or to the Web interface—no remote access is allowed:

name of user account: `user1`
access methods allowed: `Web + cli`
group membership: `admins`
assigned password: `test123`

NOTE: This example is shown in interactive mode. For more information, see **"Interactive Mode" (page 82)***.*

Enter the following commands:

```
> config user account user1
  Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
  TAB to cycle parameter options
user-accounts-user#> access web + cli
user-accounts-user#> group1 admins password test123
user-accounts-user#> exit
*> save
```

Show User Account

To show the settings for account **user1**, enter the following command:

```
> show user account user1
```

The display is similar to the following:

```
Users:
Name       Access         Auth Group1 Group3 Group5 Password
Inherit                          Group2 Group4     Enabled
-------------------------------------------------------------
user1      web + cli      SHA  admins               ******
yes                                                     yes
```

Note: Every password is encrypted, so the **Password** *field can only show asterisks.*

Deleting a User Account

To delete a user account, specify the name of the account on the command **delete user account**.

NOTE: You cannot remove or rename the predefined user accounts **admin** *and* **user.**

For example, to delete a user account named **user1**, enter the following commands:

```
> del user account user1
*> save
```

User Groups

Before you add a new user group or change an existing user group, review the settings of the current user groups by entering the following command:

```
> show user groups
```

Then, to add or change a group, use the following command:

```
> config user group
```

NOTE: The maximum number of user groups that you can define for the BSGX4e unit is 10.

Table 17 describes the parameters for `config user group`.

Table 17. User Group Configuration Parameters

Parameter	Description
[name]	Name of the user group to be added or the existing user group to be changed. This parameter is required. If an existing user group is specified, only the specified parameter values are changed; all other existing values for the group remain unchanged.
access	Access methods allowed to user accounts in this group. The default is **none**. *NOTE: A user account uses this **access** value only if its own **access** value is **none** and the access values of any preceding groups in its group list are also **none**.* **all** All access methods allowed. **none** No access allowed. You can specify that two or more of the following methods are to be connected by using plus (**+**) symbols. **ssh** Secure Shell (SSH) access allowed. **Web** Web User Interface (Web UI) access allowed. **cli** Command Line Interface (CLI) access allowed. **telnet** Remote access through a Telnet session allowed. **ftp** File Transfer Protocol (FTP) access allowed.

Table 17. User Group Configuration Parameters (continued)

Parameter	Description
auth	Internal or external password authentication. The default is internal Strong Password Hashing (**SHA**). To require external authentication, specify **RADIUS** or **TACACS** and configure an authentication record for this user account. For more information, see *"Radius Authentication" (page 68)*.
all	Indicates whether all access is given to the group. The default is **no**, meaning that enforcement is in place to check the access rights of the users in the group. If **yes** is specified for a group (such as for the **admins** group), access checks are not enforced.

Add User Group Example

This example adds a new user group as follows:

name: dev
access: all (ssh, web, cli, telnet, ftp)
all access: yes (allowed)

To add the new group, enter the following commands:

```
> config user group dev access all all yes
*> save
```

Show a User Group

To show the settings for group **dev**, enter the following command:

```
> show user group dev
```

The display is similar to the following:

```
Groups:
Name           Access                              Authorization
Allow All
-------------------------------------------------------------------
dev            ssh + web + cli + telnet + ftp      SHA
yes
```

Deleting a User Group

To delete a user group, specify the name of the group by using the command **delete user group**.

NOTE: You cannot delete the predefined user groups named **users** *and* **admins***.*

For example, to delete a user group named **dev**, enter the following commands:

```
> del user group dev
*> save
```

User Rights

This section describes how to configure a record that defines the access of a group to certain objects. The available access rights are read, write, and execute. Read allows the viewing of data; write allows the writing of data; execute is not currently used.

A group can have more than one rights record defined for it. For example, the predefined rights records **useradv** and **userbasic** are both defined for the same user group: the user group **users**. In this case, two rights records are defined so that the user group can be granted different access to different objects in the system, as follows:

- The **useradv** record applies to objects that belong to **Admins**; it grants only read access.
- The **userbasic** record applies to objects that belong to **Users**; it grants both read and write access.

NOTE: In most cases, the default user rights records should suffice; do not change them unless the effects of authority and object ownership are clearly understood.

Command Authority

Commands are objects that belong to either **Admins** or **Users**. When you list the online help for a command (by entering the command followed by a question mark (?) or tab key), you see a line for **Authority**, for example:

```
> ping?
Command:    ping
Desc:       Ping another device on the network
Authority:  Users
```

If the **Authority** is **Users**, the command is an object that belongs to **Users,** and the right to use that command is governed by the rights record that grants access to objects belonging to **Users**.

In general, commands that require write access, such as **config** commands, have **Admins** authority. Commands that only display data, such as **show** and **stats**, have **Users** authority. Similarly, maintenance commands that require write access have **Admins** authority.

The notable exception is the *save* command that saves configuration changes; it has **Users** authority so it is available to all users belonging to groups **admins** or **users**.

Configuration Requirements

You must configure the user group before you can configure a rights record for it. For more information, see *"User Groups" (page 64)*.

NOTE: In most cases, the default settings provide the appropriate permissions per user level. It is recommended not to change the settings unless

deemed necessary and only when the effects of authority and object ownership are clearly understood.

Configuration Command

Before adding a new rights record or changing an existing rights record, review the current records by entering the following command:

```
> show user rights
```

Then, to add or change a rights record, use the following command:

```
> config user rights
```

Table 18 describes the parameters for `config user rights`.

Table 18. User Rights Parameters

Parameter	Description
[id]	Identifier of the new or existing rights record. This parameter is required. If you edit an existing rights record, only the values specified on this command are changed; all other values in the record remain unchanged.
access	Rights granted by this record. **all** Read, write, and execute. **none** No rights granted. You can specify that two or more of the following methods are to be connected by using plus (**+**) symbols. **read** Read permission. **write** Write permission. **execute** Execute permission.
gname	Name of the user group granted the rights in this record.
object	Objects to which this record applies (**Admins** | **Users**). Objects can belong to Admins or to Users. For example, if the help description for a command lists its Authority as Admins, then a rights record for Admins determines if the group can use that command. For more information, see "Command Authority" (page 66).

Add User Rights Example

This example defines a new rights record. The new record applies to the user group **users**; it grants read access to objects belonging to **Users**, as follows:

id: `user` (user being configured)
access modes allowed: `read`
group name: `users`
object name: `Users`

Enter the following commands:

```
> config user rights user access read gname users object Users
*> save
```

Show User Rights Record

To show the rights record named **user**, enter the following command:

```
> show user rights user
```

The display is similar to the following:

```
Access Rights:
Identifier      Access mode     Group name Object name
-------------------------------------------------------------
user            read            users      Users
```

Deleting a User Rights Record

To delete a user rights record, specify the name of the record on the command **delete user rights**.

NOTE: You cannot rename or delete the predefined rights records named **admin**, **useradv**, *and* **userbasic**.

For example, to remove a user rights record named **user**, enter the following command:

```
> del user rights user
*> save
```

Radius Authentication

To provide additional security for user logins to the BSGX4e device, you can require an external authentication of passwords. When a password is externally authenticated, a client in the device sends the password to an external server for authentication.

The Radius client:

NOTE: When external authentication is used for a user account, the external server defines the password required for logon using the account. The **password** *command can change the internal password stored for the account, but this password is not used for authentication and so the effective password is not changed.*

The Radius client in the BSGX4e device:

- is compatible with standard Radius servers
- maps Radius authentication records to users by their user account name
- can reference up to twenty Radius authentication records

- provides legacy authentication, which enables the BSGX4e to function as a Network Access Server (NAS)

NOTE: The password of a user account is externally authenticated by a Radius server only if its **auth** *parameter value is* **Radius***. This value can be specified for the user account or for a user group to which the user account belongs. User account configuration is described on page 61 and user group configuration is described on page 64.*

Configuration Requirements

For a user account to use Radius authentication, the following requirements must be met:

1. The authentication (**auth**) value for the user account must be **RADIUS**. (User account configuration is described on page 61.)
2. The Radius client must have an authentication record for the user account.
3. The user account and its password must be defined on the external Radius server.

Configuration Steps

To configure a user account to use Radius authentication, perform these steps:

1. Change the authentication (**auth**) value for the user account to **Radius**. (User account configuration is described in "User Accounts" (page 61))
2. Configure a Radius authentication record for the user account.
3. Configure the user account and its password on the external server.

*NOTE: Disabling its authentication record suspends Radius authentication for a user account. This prevents logons by the user account until either its authentication record is reenabled or its authentication method (***auth** *value) is changed.*

Radius Authentication Records

After you configure a user account to use Radius authentication, you must configure a Radius authentication record for that user account. Every user account that uses Radius password authentication must have its own Radius authentication record.

NOTE: You must configure the user account before you configure the corresponding Radius authentication record. For more information, see **"User Accounts" (page 61)***.*

Each user account that is to use Radius password authentication must have *its own* Radius authentication record. If the same Radius server is referenced by every user account, the same values are specified in every authentication record.

NOTE: Deleting the user account also deletes its authentication record.

The Radius authentication record specifies:

- the name or address of the Radius server (**authserver**)
- the secret that the client shares with the server (**secret**)
- how the Radius server accesses the Radius client:
  - If DHCP is enabled, specify that the client automatically binds to an interface (**auto yes**) and specify the interface (**interface**).
  - If DHCP is disabled, specify the binding IP address of the client (**bindaddr**).

To configure a Radius authentication record, enter the following command:

```
> config radius client
```

Table 19 describes the parameters for **config radius client**.

Table 19. Radius Authentication Record Parameters

Parameter	Description
[user]	Name of the user account to which the authentication record applies. The user account must specify **Radius** authentication.
enabled	Indicates whether the Radius client is enabled for the user. The default is **yes**.
auto	Indicates whether the client automatically binds to the interface specified by the **interface** parameter. Specify **yes** if DHCP is in use. The default is **no**.
authserver	FQDN or IP address of the Radius authorization server that the client references.
secret	Shared secret for the client as determined by the server.
bindaddr	Binding IP address for the client. It is the IP address of the interface that the server references (typically, the IP address of the WAN interface.) Specify this value only if DHCP is *not* in use.
interface	Physical interface through which Radius communicates if the **auto** parameter is **yes.** This is typically the WAN interface (**eth0**). To clear the parameter, specify **none**.

Example of Configuring a Radius Authentication Record

This example creates an authentication record for user account **RadiusUser**. It assumes the following:

- The user account **RadiusUser** is configured and specifies **Radius** as its authentication method.
- DHCP is in enabled for the unit:

  User account name: RadiusUser
  FQDN of Radius server: radius.wan.com
  Shared secret: Radsecret
  Interface that the server references: eth0

1. Enter the following command:

```
> conf radius client RadiusUser
Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
                           TAB to cycle parameter options
radius-cl-user#> enabled yes
radius-cl-user#> auto yes
radius-cl-user#> authserver radius.wan.com
radius-cl-user#> secret Radsecret
radius-cl-user#> interface eth0
radius-cl-user#> exit
```

2. To save the configuration, enter:

```
*> save
```

Show Radius Authentication Records

To list the Radius authentication records, enter:

```
> show radius client
```

The following display shows two authentication records: one for user account **RadiusUser** and the other for user account **RadiusUser2**. Both records reference the same Radius server through the same interface (**eth0**).

```
Radius Client:

User        Enabled Auth          Bind      Interface  Automatic  Secret
-------------------------------------------------------------------------
RadiusUser  yes     172.16.1.72   0.0.0.0    eth0      yes        Radsecret
RadiusUser2 yes     172.16.1.72   0.0.0.0    eth0      yes        Radsecret
```

Radius Activity Logs

Radius client activity is reported in the system log.

To see the system log entries, enter the following command:

```
> show logging internal
```

The following display shows log entries for a failed Radius authentication:

```
(E)02:36:31: rc_send_server: bind: radius.wan.com: errno = 0x31
(C)02:36:31: RADIUS Authentication failure
(E)02:36:31: Cannot authenticate Radius!
(C)02:36:31: Cannot initialize Radius user: RadiusUser
(E)02:36:31: Cannot authenticate RADIUS user RadiusUser
(W)02:36:31: RadiusUser INVALID LOGON at TUE MAR 06 02:34:45 2007
```

TACACS+ Authentication

To provide additional security for user logins to the BSGX4e device, you can require external authentication of user logins. When a login is externally authenticated, a client in the device sends the login information to an external server for authentication.

One external authentication method uses the TACACS+ protocol. This protocol provides authentication, authorization, and accounting services. Normal operation fully encrypts the body of the packet for secure communication. It uses TCP port **49**.

The TACACS+ client:

- Is compatible with standard TACACS+ servers.
- Maps TACACS+ authentication records to users by their user account name.
- Can reference up to twenty TACACS+ authentication records.
- Provides legacy authentication, enabling the BSGX4e to function as a Network Access Server (NAS).

Configuration Steps

To configure a user account to use TACACS+ authentication, perform these steps:

1. Change the authentication (**auth**) value for the user account to **TACACS+**. This value can be specified for the user account or for a user group to which the user account belongs. (User account configuration is described in "User Accounts" (page 61) and user group configuration is described in "User Groups" (page 64).)
2. Configure a TACACS+ authentication record for the user account.

*NOTE: Disabling its authentication record suspends TACACS+ authentication for a user account. This prevents logins by the user account until either its authentication record is re-enabled or its authentication method (***auth***) is changed.*

TACACS+ Authentication Records

After a user account is configured to use TACACS+ authentication, a TACACS+ authentication record must be configured for that user account.

NOTE: The user account must be configured before the corresponding TACACS+ authentication record is configured **(***see* **"User Accounts" (page 61))**.

Each user account that is to use TACACS+ password authentication must have *its own* TACACS+ authentication record. If the same TACACS+ server is referenced by every user account, the same values are specified in every authentication record.

The TACACS+ authentication record specifies:

- the name or address of the TACACS+ server (**server**).
- the key that the client shares with the server (**key**).

To configure a TACACS+ authentication record, enter the command:

```
> config tacplus client
```

Table 19 describes the parameters for **config tacplus client**.

Table 20. TACACS+ Authentication Record Parameters

Parameter	Description
[user]	Name of the user account to which the authentication record applies. The user account must specify **TACACS+** authentication.
enabled	Whether the TACACS+ client is enabled for the user. The default is **yes**.
server	IP address of the TACACS+ server that the client references.
key	Shared key for the client as determined by the server.

Example of Configuring a TACACS+ Authentication Record

This example creates an authentication record for user account **TACuser**. It assumes that the user account **TACuser** has been configured and **TACACS+** has been specified as its authentication method.

User account name: TACuser
IP address of TACACS+ server: 172.16.249.52
Shared key: tacacskey

Enter these commands:

```
> config tacplus client TACuser

Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
                           TAB to cycle parameter options
tacplus-cl-user#> enabled yes
tacplus-cl-user#> server 172.16.249.52
tacplus-cl-user#> key tacacskey
tacplus-cl-user#> exit
*> save
```

Show TACACS+ Authentication Records

To list the TACACS+ authentication records, enter:

```
> show tacplus client
```

The following display shows two authentication records, one for user account **TACuser** and the other for user account **root**. Both records reference the same TACACS+ server.

```
TACACS+ Client:

User         Enabled Server         Key
-------------------------------------------------------------
TACuser      yes     172.16.249.52  tacacskey
root         yes     172.16.249.52  tacacskey
```

TACACS+ Activity Logs

TACACS+ client activity is reported in the system log. Log entries indicate whether authentication attempts are successful or not.

To see the system log entries, enter the following command:

```
> show logging internal
```

The following display shows log entries for a failed TACACS+ authentication:

```
(I)22:16:24: User root is attempting to logon at THU FEB 08 22:16:24 2007
(I)22:16:24: Verify TACACS+ user root at THU FEB 08 22:16:24 2007
(I)22:16:24: User root cannot be found
(C)22:16:24: Cannot authenticate Tacacs+ user: root
(W)22:16:24: root INVALID LOGON at THU FEB 08 22:16:24 2007
```

TACACS+ Authentication

To provide additional security for user logins to the BSGX4e device, you can require external authentication of user logins. When a login is externally authenticated, a client in the device sends the login information to an external server for authentication.

NOTE: When external authentication is used for a user account, the external server defines the password required for logon using the account. The **password** *command can change the internal password stored for the account, but this password is not used for authentication and so the effective password is not changed.*

One external authentication method uses the TACACS+ protocol to provide authentication services. Normal operation fully encrypts the body of the packet for secure communication. It uses TCP port **49**.

The TACACS+ client in the BSGX4e device:

- Is compatible with standard TACACS+ servers.
- Maps TACACS+ authentication records to users by their user account name.
- Can reference up to twenty TACACS+ authentication records.
- Provides ASCII login authentication, enabling the BSGX4e to function as a Network Access Server (NAS).

Configuration Requirements

For a user account to use TACACS+ authentication, the following requirements must be met:

1. The authentication (**auth**) value for the user account must be **TACACS+**. (User account configuration is described on page 61.)
2. The TACACS+ client must have an authentication record for the user account.

3. The user account and its password must be defined on the external TACACS+ server.

*NOTE: Disabling its authentication record suspends TACACS+ authentication for a user account. This prevents logins by the user account until either its authentication record is re-enabled or its authentication method (***auth** *value) is changed.*

TACACS+ Authentication Records

For each user account configured to use TACACS+ authentication, a TACACS+ authentication record must be configured. The authentication record for a user account serves two purposes:

- It specifies the TACACS+ server that authenticates the account by providing:
  - the name or address of the TACACS+ server (**server**).
  - the key that the client shares with the server (**key**).
- It enables or disables TACACS+ authentication for the account.

NOTE: Deleting the user account also deletes its authentication record.

Every authentication record that references the same TACACS+ server specifies the same **server** and **key** values.

To configure a TACACS+ authentication record, enter the command:

```
> config tacplus client
```

Table 21 describes the parameters for **config tacplus client**.

Table 21. TACACS+ Authentication Record Parameters

Parameter	Description
[user]	Name of the user account to which the authentication record applies. To use the authentication record, the user account must specify **TACACS+** authentication.
enabled	Whether the TACACS+ client is enabled for the user. The default is **no**.
server	IP address or FQDN of the TACACS+ server that the client references.
key	Shared key for the client as determined by the server. If the key includes a space character, enclose the key value in double-quote characters(“ “)

Example of Configuring a TACACS+ Authentication Record

This example creates an authentication record for user account **TACuser**. It assumes that the user account **TACuser** has been configured and **TACACS+** has been specified as its authentication method, as shown in the following display:

```
> show user account TACuser
Users:
Name       Access                    Auth Group1 Group3 Group5 Password
Inherit                                   Group2 Group4        Enabled
-------------------------------------------------------------------------
TACuser    ssh + web + cli + telnet  TAC* admins               ******
yes                                                           yes
```

4 COMMAND INTERFACE

This chapter describes the Command Line Interface (CLI) for the BSGX4e device. The CLI provides commands for every function of the device. It also provides online help and an interactive mode for easier command entry.

For an introduction to the other user interface, the Web User Interface, see *"Web User Interface" (page 379)*.

This chapter discusses these topics:

- Command entry.
- Logging out.
- Customizing the command session.
- Saving configuration changes across restarts.
- Defining commands that are automatically run at restart.
- Getting online help.
- Command syntax.
- Maintenance commands.
- Debug commands.

Command Entry

This chapter assumes that the BSGX4e device is installed in a working network as described in the *BSGX4e Installation Guide*. It also assumes that you can log on to the device from a terminal session at your workstation or a console.

After you log on to the BSGX4e unit from a terminal session, you see a command prompt. The command prompt consists of a string followed by the greater than (**>)** symbol. You can customize the string as described in the next section. Therefore, the convention in this guide is to show the command prompt as just the **>** symbol:

```
>
```

You can enter any command in response to this prompt. However, if you logged in with a user ID that does not have authority to execute the command, the unit responds as in the following example:

```
> reboot
Invalid access for user 'user'!
```

For more information about the authority granted to user accounts, see *"User Accounts, Groups and Rights" (page 61)*.

The Command Line Interpreter executes a command as soon as it receives it.

- If the entire command is entered on one line, the command is executed immediately after the <**enter**> key is typed.
- If the command is entered in interactive mode (see "Interactive Mode" (page 82)), the command is executed as soon as its entry is complete (after entry of **exit** or <**cntrl-z**>).

NOTE: Although **config** *commands change the current configuration immediately, the changes can be lost if the unit restarts. To save the changes to permanent memory, enter a* **save** *command.*

Logging Off

A session begins with a logon using a valid user account and password. The session ends when:

- An **exit** command is entered, or
- The session inactivity timer expires. By default, a session expires after five minutes of inactivity (see "Customizing the Command Session" (page 78)).

Exit Command

The exit command ends the session without saving configuration changes to nonvolatile memory. Assuming the unit does not restart, the configuration remains the same at the next logon, including the changes that were not saved by the last session.

In the following example, asterisks in a command prompt indicate that changes have not been saved. The **exit** command ends the current session; the logon starts a new session. The command prompt in the new session still has asterisks, showing that configuration changes have not been saved:

```
*BSGX4e*> exit
Logging off
User logout. Goodbye!

User: nnadmin
Password:

*BSGX4e*>
```

Customizing the Command Session

You can change any of the following terminal settings:

- line width (initially, 80 characters)
- command prompt
- session timeout (initially, 60 minutes)

To see the current terminal settings, enter the following command:

```
> show shell terminal

Terminal Settings:

   Width        80
   Prompt       BSG
   Timeout      60 (min)
```

Changing the Terminal Settings

To change the terminal settings, use the following command:

```
> config shell terminal
```

Table 22 lists the terminals parameters:

Table 22. Terminal Session Parameters

Parameter	Description
width	Number of characters in a terminal line. The initial value is 80 characters.
prompt	Character string used in the command prompt. The initial value is BSGX4e.
timeout	Number of minutes before the terminal session automatically logs out. The default is five minutes.

Example of a Command Prompt Change

The following command changes the command prompt from BSGX4e to BSG:

```
BSGX4e> config shell terminal prompt BSG
*BSG*> save
BSG>
```

Saving Configuration Changes

The Command Line Interpreter executes each command immediately after it is entered. A change specified by a configuration command is applied immediately to the current configuration. However, the change is not made to the configuration stored in nonvolatile memory. Thus, unstored configuration changes are lost if the unit restarts.

To save the current configuration (and any unstored changes) to nonvolatile memory, enter a save command.

To remind you that configuration changes are pending, the command prompt changes so it contains asterisks. For example, the default command prompt changes from **BSGX4e>** to ***BSGX4e*>**. The asterisks indicate that, although received and applied, the entered changes are not yet stored in nonvolatile memory.

By convention, this guide shows the command prompt with asterisks as just ***>**. For example, the **save** command is entered after a ***>** prompt:

```
*> save
Saving:.:.:.
```

For example, the following commands cause the unit to display its system information immediately after each restart:

```
> config system startup 0 command “show system info”
*> save
```

Online Help

To get online help with commands while logged in to the device, use the command **help.**

General Help

To list general information about the CLI, type the word **help** after a command prompt and press the enter key:

```
> help
```

A long list is displayed. First, all commands are listed under the following headings:

```
Maintenance Commands:
Debug Commands:
Command Groups (CLI commands):
```

Then, there is a description of how to get more specific command help for maintenance and debug commands:

```
Maintenance Commands:
Type the name of any of the maintenance commands to execute
it. You can also use the '?' to bring up help at any time.
This will display context help or help on the various
parameters. For example, 'cp ?' to display help information
for the 'cp' maintenance command.

Debug Commands:

The debug commands become available by entering 'debug
enable.' (They are disabled by default.) Once enabled, type
the name of the debug command to execute it. You can also use
the '?' to bring up help on the debug commands. For example,
'emac ?' to display help information for the 'emac' debug
command.
```

Finally, a description of the CLI command syntax and how to get custom help appears:

```
Prefixes:
Variables:
```

Specific Help

For specific information about a command, you can either:

- Specify the command by using the **help** command.
- Enter part of the command followed by the **Tab** key or the question mark (**?**) key.

An example follows:

- **For information about the command to configure an IP interface, enter any of the following:**

  ```
  > help config interface ip
  ```
  or
  ```
  > config interface ip ?
  ```
  or
  ```
  > config interface ip <TAB>
  ```

  In response to any of those entries, the online help display lists the parameters for **config interface ip,** as follows:

  ```
  [if]          Interface to change behaviour of (eth0 | eth1)
  ip            IP address and mask of interface
  mtu           The Maximum Transmission Unit (MTU) of the
                interface
  dhcp          Whether or not DHCP is enabled for the
                interface
  status        Configuration status of the interface (up |
                down)
  speed         Speed/Duplex of eth0 (Auto | 10Half | 10Full |
                100Half | 100Full)
  ```

Interactive Mode

You can use the interactive mode to enter a command on one line or split the command between two or more lines. With a single line entry, type the command with all its parameters before you press <**enter>**. In interactive mode, enter the command on one line, but enter its parameters on one or more following lines.

Interactive mode is provided for most CLI commands. Some commands require that you enter the command and its *primary key* on the first line. The primary key is the object of the command, such as a user account name. In the parameter lists in this guide, a primary key parameter is shown in brackets.

To get help while in the interactive mode, enter a question mark (**?**).

In the following example, the command **config security nat policy** and its primary key **new** is entered on the first line, and then its parameters are entered on following lines:

```
> config security nat policy new
Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
                           TAB to cycle parameter options
nat-pol-new#> type port
nat-pol-new#> address 10.0.1.130
nat-pol-new#> port 2600
nat-pol-new#> exit
```

NOTE: The command prompt changes while in the interactive mode.

NOTE: To leave the interactive mode, enter **exit** *or the key combination* **ctrl-z** *to execute the command, or enter* **quit** *or the key combination* **ctrl-c** *to cancel the command.*

CLI Command Syntax

The following syntax applies to CLI commands:

```
<prefix> <command group> <command sub-group> [<primary key>]
{[no] [<parameter>] [<value>]}
```

NOTE: Square brackets ([ ]) indicate one or no occurrence, and braces ({ }) indicate one or more occurrences.

The command **prefixes** are:

- `config` Configure an object's variables.
- `display` Display the current configuration of an element.
- `del` Delete an element.
- `show` Show the current active information about an element.
- `stats` Show statistics about an element.
- `clear` Clear statistics for an element.

If you enter a command prefix followed by a ?, all **command groups** are listed. For example, if you enter **`config?`**, one of the command groups listed is **`ids`**.

Some command groups have **command sub-groups**. To see a list of its sub-groups, enter the prefix and the command group following by a ?. For example, to see the sub-groups for **`config ids`**, enter:

```
> config ids?
ids anomaly                        Anomaly based IDS prevention
ids flood activity                   IDS Flood protection
ids flood settings                   IDS Flood protection
ids scan                             IDS Scan protection
ids spoof                            IDS spoofing protection
> config ids
```

Finally, to see the parameters for a command, enter the command sub-group followed by a ?.

```
> config ids spoof?

[name]              Name of the interface (eth1)
type                Whether its a trusted or untrusted
                    interface (trusted | untrusted)

> config ids spoof
```

Notice that the first parameter, [name], is bracketed, indicating that it is a primary key.

Parameter Values

In general, a parameter is specified by its name followed by its value. For example, port 2600 specifies the value 2600 for the *port* parameter.

The following list describes exceptions for specifying parameter values:

- **Primary Key**

  If the first parameter for a command is listed in brackets (such as [name]), it is a primary key parameter and specifies the object of the command. The primary key value is specified without its parameter name.

  For example, the first parameter of the command **config ids spoof** is listed as **[name]** and the second parameter as **type**. When you enter the command, specify just the value for the first parameter, but both the name and its value for the second parameter.

  > **config ids spoof eth1 type trusted**

- **Booleans**

  Boolean parameters are parameters with just two states (on/off or yes/no). To specify the *on/yes* state, specify only the parameter name and omit any value. To specify the *off/no* state, specify the keyword **no** followed by the parameter name.

  For example, the following command specifies the *on/yes* state for the **enabled** parameter:

  > **config user account user1 enabled**

  To specify the off/no state for the **enabled** parameter, specify:

  > **config user account user1 no enabled**

- **IP address ranges**

  When you specify an IP address range, use a hyphen between the first and last addresses of the range (**192.16.1.20-192.16.1.25**) or use a subnet mask suffix (**192.168.1.1/24**).

- **Numeric offsets**

  Certain numeric parameters use a plus (**+**) or a minus (**-**) symbol before the numeric value to indicate an offset. For example, to configure a gain of -5, use:

  > **config voice parameters gain -5**

Command Keyword NO

The keyword **no** is used to turn off a Boolean parameter or to clear string parameters (to fill the string value with blanks).

NOTE: You must enter the **no** *keyword* **before** *the parameter identifier.*

For example, the following command turns off the Netflow agent by turning off the Boolean parameter **enabled**:

```
> config netflow agent no enabled
```

As an example of using **no** to clear a string parameter, the following command clears the name of the unit. (The default unit name is MyUnit.)

```
> config system info no unit
```

To see the result, enter:

```
*> show system info
```

The Unit Name is now blank:

```
System Info:

    Unit Name
    Bootcode Ver    1.1.0.01B-0001
    App. Ver        2.020.01382-01B-0007
    System Type     40BSGX4e
    Memory          97/128 MB
    MAC 0           00:22:11:44:33:04
    MAC 1           00:22:11:44:33:05
    Serial          A628000003
    Country         United States of America (US)
    Temp            Unsupported
    Up time         0y 0d 4h 33m 20s
```

Command Keyword ALL

Use the keyword **all** to perform the command on all entries. The command action can be modification, deletion, clearing of statistics, or display.

NOTE: You must enter the **all** *keyword* **before** *all parameters.*

For example, the following command changes the specified parameter for *all* QoS Quality Groups. (It changes the **iptos** parameter value to 248.)

```
> config qos group all iptos 248
```

To see the result, enter:

```
*> show qos group all
QoS Quality Groups:

Name        Link  QG    Type     Committed  Burst     IPToS COS
-------------------------------------------------------------
Management  eth0  A2    car      1000000    100000000  248   no
VoIP        eth0  A1    policed  89000000   0          248   no
```

As another example, the following command deletes *all* QoS Quality Groups:

```
> del qos group all
```

Maintenance Commands

To see a list of available maintenance commands, enter the **help** command. The maintenance commands are also listed at the end of this section.

Maintenance Command Syntax

Maintenance commands have the following syntax:

```
<maintenance command> {[<parameter>] [<value>]}
```

NOTE: Square brackets ([ ]) indicate one or no occurrence, and braces ({ }) indicate one or more occurrences.

Maintenance Command Help

For information about a specific maintenance command, enter the command, followed by a question mark **(?)**or the **tab** key.

For example, the following command lists information about the **ping** command:

```
> ping?
Command:    ping
Desc:       Ping another device on the network
Authority:  Users

Usage: ping destination [-c count] [-t timeout] [-i interval]
       [-l preload] [-f][-p pattern] [-s packetsize] [-q]

Options:
    -c count      number of ping requests to send, '-c' means
non-stop
    -t timeout     total time (sec) before ending ping
requests. '-t' means non-
stop
    -i interval    time interval (msec) between ping requests
    -l preload     initial number of ping requests to send
    -f             flood ping
    -p pattern     pattern to use
    -s bytes       number of data bytes to send
    -q             completely quiet during ping
```

List of Maintenance Commands

The following list of maintenance commands is divided into two lists:

- The first list is for commands that require only Users authority so that anyone can use them.
- The second list is for commands that require Admins authority. To use these commands, log on with a user ID that has administrator authority (such as **nnadmin**).

Commands that Require Only Users Authority

Command	Purpose
arp	Show or flush the ARP table, or set/delete static arp entries
cat	Display files
cd	Change to another directory
cls	Clear the terminal screen
cp	Copy a file
cpu	Show details on CPU and AP usage
dump	Dump the current configuration as a re-entryable script
logoff	Log off the system
ls	List the file system
mkdir	Make directories
netstat	List current networking connections and listening ports
password	Change the specified user's password
ping	Ping another device on the network
pwd	Print name of current/working directory
rm	Remove files/directories
route	Modify/display the static IP routing table
save	Save the current configuration to permanent storage
summary	Provide summary of current system performance and state
tech-support	Display system information useful to technical support staff
time	Display / set the system time
traceroute	Trace the route to another device on the network
uptime	Display the uptime of the system

Commands that Require Admins Authority

Command	Purpose
debug	Enable additional debug commands for diagnosing faults
dosfs	Manage the DOS file system
erase	Erase the current configuration from permanent storage
reboot	Restart the system
reload	Reload the system
tcpdump	Display network traffic
telnet	User interface to remote host using TELNET protocol
whoison	Display who is on and where they are from

Debug Commands

A set of debug commands provides access to additional information for debugging purposes.

NOTE: All debug commands (and the command that enables debug mode) require **Admins** *authority. To access debugging information, you must log on with a user ID that has administrator authority* **(such as nnadmin)**.

To see a list of available debug commands, enter the **help** command. The debug commands are also listed at the end of this section.

Debug commands are available in debug mode only. To begin debug mode, enter:

```
> debug enable
```

To end debug mode, enter:

```
> debug disable
```

NOTE: Debug mode can slow operations. Remember to exit debug mode as soon as possible.

Debug Command Syntax

Debug commands have the following syntax:

```
<debug command> {[<parameter>] [<value>]}
```

NOTE: Square brackets ([ ]) indicate one or no occurrence, and braces ({ }) indicate one or more occurrences.

Debug Command Help

For information about a specific debug command, enter the command followed by the **tab** key or question mark (**?**). An example follows.

For example, the following command lists information about the **basemac** command:

```
> basemac?
Command:    basemac
Desc:       Set up the base MAC address for Ethernet controllers
Authority:  Admins

Usage: basemac AA:BB:CC:11:22:33
```

List of Debug Commands

NOTE: All debug commands (and the command that enables debug mode) require **Admins** *authority. To access debugging information, you must log on with a user ID that has administrator authority (such as* **nnadmin**).

Command	Purpose
apread	Read from the AP memory

```
apgos         Debugging information about AP GoS
apids         Display information about AP-IDS
aplookup      Look up symbol in AP DMEM symbol table
apmode        Configures AP0 as eth0apreadRead from the AP
               memory
apregs        Display the current AP registers
apwrite       Write to the AP memory
basemac       Set up the base MAC address for Ethernet
              controllers
bcmchip       Print the broadcom switch chip revision
collision     Display collisions in RFT table
connections   Display firewall connection information
devs          Display information about devices
dspread       Read from the DSP memory
dsptest       Start and stop test actions on a DSP channel
dsptone       Toggle tones on a particular channel
dspwrite      Write to the DSP memory
dumpcmd       Display all commands available in system
emac          Display debug emac stats
flash         Format the compact flash
fxo           FXO testing code
fxs           FXS testing code
gosstats      Test gos stats for Web
i2cscan       Scan the I2C bus for devices
initfunc      Displays the function at the n'th dot from the
               boot sequence
jbshow        Show new jitter buffer stats
ledflash      Flashes the LED on the front of the unit
memory        Displays information about the memory/buffers
mib           Displays or extracts the built in autogenerated
               MIBs
mii           Read/write MII registers
nfsmount      Mount a remote NFS volume
scanblocked   Display IP addresses blocked by IDS
stack         Current running tasks stack information and
              state
tasks         Display currently running tasks and change their
              priorities
temp          Read/write temperature sensor registers
thrash        Run the bus thrashing tests
trustedlist   Display IDS Trusted List Table
tt            Display stack trace - can't be applied to the
              task itself
vqmt          Send vqm trap
```

5 WAN INTERFACE CONFIGURATION

This chapter describes how to configure the data interface that connects the BSGX4e unit to an external network, or WAN. The WAN interface in the BSGX4e is an Ethernet interface referenced as eth0. It provides a bandwidth of 100 Mbps.

Ethernet WAN Port and Interface

The Ethernet WAN settings include both speed and duplex mode for the WAN port, and IP address settings for the WAN interface. To initialize network communication during the installation of the unit, the WAN port and interface may already be configured. To see the current configuration settings for the WAN port and interface, enter the following command:

```
> show interface ip eth0
```

The display is similar to the following:

```
"eth0" info:

   Interface           eth0
   Flags               (8843) < UP BROADCAST RUNNING SIMPLEX MULTICAST >
   IP Address/Mask     0.0.0.0/255.0.0.0
   MTU                 1500
   DHCP                on
   Lease obtained      N/A
   Lease expires       N/A
   MAC Address         00:19:09:74:00:00
   Speed               FULL100
   Configured Speed    AUTONEG
```

WAN Ports

The Ethernet interface actually provides two ports to the WAN, identified as follows:

- **mii0**: uplink to the IP host
- **eth0**: front WAN port

You cannot configure the uplink port (mii0). It always operates at 100 Mbps, full duplex mode, flow control disabled.

You can configure the **eth0** port as follows:

- Its **speed** can be 10Base-T, 100Base-T, or autonegotiated. The default is autonegotiated.

- Its **duplex mode** can be half duplex, full duplex, or autonegotiated. The default is autonegotiated.

NOTE: You cannot configure the eth0 flow control setting; it is always disabled.

WAN Interface (eth0)

For traffic to be routed to the WAN interface (eth0), you must assign an IP address to it. The IP address is assigned automatically by a DHCP server if the DHCP service is enabled for the eth0 interface. Otherwise, you must assign an IP address manually.

NOTE: Initially, the eth0 interface is configured with DHCP enabled. To see the current eth0 configuration, enter the command **show interface ip eth0***.*

eth0 Configuration Command

To change the settings for the eth0 interface, enter the following command:

```
> config interface ip eth0
```

Table 24 describes the parameters for **`config interface ip eth0`**.

Table 24. eth0 Parameters

Parameter	Description
`ip`	IP address and mask of the eth0 interface. Specify an address only if DHCP is disabled. The address and mask can be specified with dotted-decimal or CIDR notation (for example, 192.168.15.3.3/255.255.255.0 or 192.168.15.33/24).
`mtu`	Maximum Transmission Unit (MTU) of the interface (in bytes). The default is **1500** bytes.
`dhcp`	Indicates whether DHCP is enabled for the interface. DHCP is initially enabled (**on**).
`status`	Indicates whether the eth0 interface is enabled or disabled (**up** | **down**). The default is **up**.
`speed`	Indicates whether the speed and duplex mode for eth0 is autonegotiated or explicitly specified. For autonegotiation, specify **auto**; otherwise, specify 10 or 100 Mbps and half or full duplex (**auto** | **10Half** | **10Full** | **100Half** | **100Full**). The default is **auto**.

Configure eth0 Example

This section provides configuration examples for the WAN front port.

Example 1

The following example shows how to configure DHCP service for the eth0 interface.

```
> config interface ip eth0 dhcp
*> save
> show interface ip eth0
"eth0" info:

   Interface         eth0
   Flags            (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP MULTICAST >
   IP Address/Mask   172.29.0.124/255.255.0.0
   MTU               1500
   DHCP               on
   Lease obtained    WED MAR 28 09:12:18 2007
   Lease expires     WED MAR 28 10:12:18 2007
   MAC Address       00:15:93:00:02:B2
   Speed             FULL100
   Configured Speed  AUTONEG
```

Example 2

The following example configures a static IP address for the WAN interface and disables DHCP service.

```
> config interface ip eth0 ip 172.29.19.10/16 dhcp off
> show interface ip eth0
"eth0" info:

   Interface         eth0
   Flags            (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP MULTICAST >
   IP Address/Mask   172.29.19.10/255.255.0.0
   MTU               1500
   DHCP              off
   Lease obtained    N/A
   Lease expires     N/A
   MAC Address       00:15:93:00:02:B2
   Speed             FULL100
   Configured Speed  AUTONEG
```

Example 3

The following example disables the WAN interface, preventing all communication with the external network. The **eth0** display then shows that the interface is down by the **DOWN** indicator on the **Flags** line.

```
> config interface ip eth0 status down
*> show interface ip eth0
"eth0" info:

  Interface         eth0
  Flags            (A842) < DOWN BROADCAST RUNNING SIMPLEX LINKUP MULTICAST>
  IP Address/Mask   172.29.19.10/255.255.0.0
  MTU               1500
  DHCP              off
  Lease obtained    N/A
```

```
Lease expires     N/A
MAC Address       00:19:09:74:00:00
Speed             FULL100
Configured Speed  AUTONEG
```

Show eth0 Configuration

To show the eth0 configuration, enter the following command:

```
> show interface ip eth0
```

The display is similar to the following:

```
"eth0" info:

  Interface          eth0
  Flags               (8843) < UP BROADCAST RUNNING SIMPLEX MULTICAST >
  IP Address/Mask    0.0.0.0/255.0.0.0
  MTU                1500
  DHCP               on
  Lease obtained     N/A
  Lease expires      N/A
  MAC Address        00:19:09:74:00:00
  Speed              FULL100
  Configured Speed   AUTONEG
```

Notice the following in the preceding display:

- The **Flags** line indicates whether the status of the interface is **UP** or **DOWN**.
- The **DHCP** line indicates whether DHCP is **on** or **off**.
- The **Lease obtained** and **Lease expires** lines display **N/A** if DHCP is off or DHCP has not assigned an IP address to **eth0**. Otherwise, the lines describe the DHCP lease for the IP address assigned.
- The **Speed** reports the current negotiated speed:
  - **FULL100** 100 Mbps, full duplex mode
  - **HALF100** 100 Mbps, half duplex mode
  - **FULL10** 10 Mbps, full duplex mode
  - **HALF10** 10 Mbps, half duplex mode
- The **Configured Speed** line reports the **speed** setting in the eth0 configuration: either **AUTONEG** (autonegotiation enabled) or a specific speed and duplex mode (**FULL100**, **HALF100**, **FULL10**, or **HALF10**).

eth0 Statistics

The device keeps statistics on the packets received and transmitted through the eth0 interface. To see the statistics, enter the following command:

```
> stats interface ip eth0
```

The following is an example of the statistics display that is provided:

```
eth0 Stats
  Tx                 344314094     Rx                423958971
  OutUnicasts        344314025     In Unicasts       423881202
  OutBroadcasts             69     InBroadcasts          57861
```

```
OutPause                    0     InPause                    0
OutMulticasts               0     InMulticasts           19908
Tx error                 3317     Rx error                  96
Deferred                    0     InDiscards                 0
Late Collisions             0     CRCErr                 75572
Collisions                  0     Jabber                    92
Excessive                   0     AlignErr                   0
Multiple                    0     Undersize                  0
Single                      0     Oversize                   0
Out Octets       97968068849     Filtered                   0
                                 Fragments
                                 InGoodOctets   350813118374
                                 In64Octets          1488666
                                 In127Octets        19993035
                                 In255Octets       193333088
                                 In511Octets         330017
                                 In1023Octets       11193721
                                 InMaxOctets        197620444
```

Clear Statistics

The following command clears the statistics kept for the eth0 interface:

```
> clear interface ip eth0
```

6
LAN SWITCH CONFIGURATION

This chapter describes how to configure the following features of the BSGX4e device:

- the **ports** of the LAN switch
- the Ethernet interface (**eth1**) to the LAN switch
- Address Resolution Logic (**ARL**) (see "ARL Configuration" (page 104))
- **layer 2 QoS** (see "Layer 2 QoS" (page 106))

The LAN switch also allows for monitoring of port traffic as described in "Port Mirroring" (page 339).

Introduction

The LAN switch in the unit implements a nonblocking switch fabric, which enables packet switching at wire speed over all ports. The LAN switch contains the following:

- The switch provides four LAN ports.
- Within the BSGX4e device, the switch passes traffic to the LAN Ethernet interface called eth1. Traffic destined for the WAN is then routed to the WAN interface.

LAN configuration requires the configuration of both the LAN ports and the LAN Ethernet interface. Configuration of the LAN interface is described in "LAN Interface (eth1)" (page 102).

LAN Switch Ports

The LAN switch provides four LAN front ports (ports 1 through 4).

The switch also has an uplink port (port 0 or MII). Network traffic from the switch is sent through port 0 to the host for processing. The uplink port cannot be configured. It always operates at 100 Mbps, full duplex mode, flow control disabled.

Speed and Duplex Mode

You can configure each front port with a specific speed and duplex mode or you can configure the port to automatically negotiate the appropriate speed and duplex mode. The possible speeds are either 10Base-T, or 100Base-T and either half or full duplex mode.

The initial configuration for each LAN port specifies **autonegotiation** for speed and duplex mode.

Flow Control

You can disable or configure flow control for a port to provide either back pressure (forced collision) for half duplex mode or pause frames for full duplex mode.

The initial configuration for each LAN port **disables** flow control.

NOTE: You cannot enable flow control if layer 2 QoS is enabled (see "Layer 2 QoS" (page 106)).

LAN Port Configuration Command

To change the configuration of a port, specify the port number on the following command:

```
> config switch port
```

Table 25 describes the parameters of **config switch port.**

Table 25. LAN Port Parameters

Parameter	Description
[port]	Port to configure (**1** to **4**).
speed	Select autonegotiation or specify a speed (10Base-T or 100Base-T) and a duplex mode (half or full) (**Auto** | **10Half** | **10Full** | **100Half** | **100Full**). The default is **Auto**.
flow	Enable flow control (back pressure [forced collision] for half duplex mode or pause frames for full duplex mode) (**yes** | **no**). The default is **no**.
enabled	Indicates whether the port is enabled (**yes** | **no**). The default is **yes**.

LAN Port Configuration Examples

This section provides examples for configuring LAN front ports.

Example 1

This example enables port 2 and changes its speed setting to autonegotiation:

```
> config switch port 2 speed auto enabled yes
*> save
```

Example 2

This example enables port 3 and changes its configuration, as follows:

Speed: `100full` (100 Mbps, full duplex)
Flow control: `yes`
Enabled: `yes`

```
> config switch port 3 speed 100full flow yes enabled yes
*> save
```

Example 3

This example enables port 4 and changes its configuration, as follows:

Speed: `10half` (10 Mbps, half duplex)
Flow control: `yes`
Enabled: `yes`

```
> config switch port 4 flow yes speed 10half enabled yes
*> save
```

Show Port Configuration

To show the current configuration of the LAN ports, enter the following command:

```
> show switch port

Switch Ports:

Port  Speed      Enabled  Flow Ctrl
-------------------------------------
0-0   Auto       yes      no
0-1   Auto       yes      no
0-2   Auto       yes      no
0-3   100Full    yes      yes
0-4   10Half     no       yes
```

In all port displays, the port is designated by its unit and port numbers, such as `0-1`, which means unit 0, port 1.

Show Port Status

To show the current status of the LAN ports, enter the following command:

```
> show switch status
```

A status line is displayed for every switch port. The following example shows the status for ports 0-4:

```
Switch Status:

Port  Link Speed/Duplex    FlowCtl
-------------------------------------------------------------
0-0    UP    100Full           None
0-1    UP    100Full           Yes-Both
0-2    UP    100Full           No-Local
0-3    UP    100Full           Yes-Both
0-4    UP    100Full           No-Local
```

The field `Flow Ctrl` shows the current flow control status of the port:

- Flow control cannot be enabled on the uplink port (`0-0`) so its value is always `None`.

- The possible `Flow Ctrl` values are:

  `None` No flow control by either the BSGX4e or its partner.
  `No-Local` Flow control by the BSGX4e, but not by its partner.
  `No-Partner` Flow control by the its partner, but not by the BSGX4e.
  `Yes-Both` Flow control by both the BSGX4e and its partner.

Show Port Statistics

The device keeps packet statistics for the LAN switch ports. You can display the statistics as a summary of statistics for all LAN ports or as detailed statistics for a specific port.

Summary of Port Statistics

To list a statistics summary for all LAN ports, enter the following command:

```
> stats switch summary
Switch Stats:


Port Rx Frames       In Good Octets  Undersize In Bad Octets
     Tx Frames       Out Octets      Oversize  Align Err
-------------------------------------------------------------
--
0-0  13052           1933600         0         0
     3348            413758          0         0
0-1  0               0               0         0
     0               0               0         0
0-2  0               0               0         0
     0               0               0         0
0-3  0               0               0         0
     0               0               0         0
0-4  3348            413758          0         0
     13050           1933553         0         0
```

Table 26 describes the statistics.

Table 26. LAN Port Summary Statistics

Statistic	Description
Port	Port unit and number. (Port 0-0 is the uplink [MII] port of the switch.)
Rx Frames	Total valid received frames.
Tx Frames	Total transmitted frames.
In Good Octets	Total data octets of received frames with valid Frame Check Sequence (FCS) (preamble not included). This count includes undersized and oversized frames.
Out Octets	Total data octets transmitted, including valid FCS (preamble not included).

Table 26. LAN Port Summary Statistics

Statistic	Description
Undersize	Total frames with length less than 64 octets, with valid FCS.
Oversize	Total frames with length greater than the maximum size, with valid FCS.
In Bad Octets	Total data octets of received frames with invalid FCS (preamble not included). This count includes jabbers and fragments.
Align Err	Total frames of a valid size, but with invalid FCS and nonintegral octets.

Detailed Port Statistics

To show the detailed statistics that are kept for a specific LAN port, specify the port number on the **stats switch port** command. For example, to see the statistics for port 1, enter:

```
> stats switch port 1

Port "0-1" stats:

Tx                  2868          Rx                  1500003
OutUnicasts            6          In Unicasts         1500000
OutBroadcasts       2850          InBroadcasts              3
OutPause               0          InPause                   0
OutMulticasts         12          InMulticasts              0
OutFCSErr              0          InFCSErr                  0
Out64Octets         2856          In 64 Octets              3
Out127Octets           0          In127Octets         1500000
Out255Octets          12          In255Octets               0
Out511Octets           0          In511Octets               0
Out1023Octets          0          In1023Octets              0
OutMaxOctets           0          InMaxOctets               0
Deferred               0          InDiscards                0
Out Octets        184392          InGoodOctets      117000192
AlignErr               0          InBadOctets               0
Oversize               0          Undersize                 0
Jabber                 0          Fragments                 0
Collisions             0          Late Collisions           0
Excessive              0          Filtered                  0
Single                 0          Multiple                  0
```

Clear Port Statistics

To clear the statistics that are kept for a LAN port, specify the port number on the **clear switch port** command. For example, to clear the statistics for port 1, enter:

```
> clear switch port 1
```

LAN Interface (eth1)

This section describes how to configure the IP interface to the LAN (eth1). The eth1 interface is the interface for the uplink (MII) port for the LAN switch. Thus, its configuration is always 100 Mbps, full duplex mode, with flow control disabled.

NOTE: Configure the LAN ports before configuring the LAN interface (eth1). See "LAN Switch Ports" (page 97).

NOTE: Initially, the DHCP client is disabled for eth1 and the static IP address 192.168.1.1/24 is assigned to the interface. To see the current eth1 configuration, enter **show interface ip eth1**.

A DHCP server is configured on the eth1 interface. When a LAN device requests an IP address, the DHCP server can assign an address from its address pool. For more information, see "DHCP Server" (page 309).

eth1 Configuration Command

To configure the IP interface for the LAN, enter the following command:

```
> config interface ip eth1
```

Table 27 describes the parameters for **config interface ip eth1**.

Table 27. LAN Interface Parameters

Parameter	Description
ip	IP address and mask of interface. The address and mask can be specified with dotted-decimal or CIDR notation (for example, 192.168.15.3.3/255.255.255.0 or 192.168.15.33/24). This parameter is required if DHCP is disabled. The subnet must not overlap with that of any other interface or include addresses from the DHCP server pool (see "DHCP Server" (page 309)).
mtu	Maximum Transmission Unit (MTU) of the interface (in bytes). The default is **1500** bytes.
dhcp	Indicates whether DHCP is enabled. The initial setting is **off**.
status	Indicates whether eth1 is enabled (**up** | **down**). The default is **up**.

Configure eth1 Interface Example

The following example specifies the IP address and mask of the eth1 interface and then saves the configuration:

IP address: 192.168.1.1
IP mask: 255.255.255.0

Enter the following commands:

```
> config interface ip eth1 ip 192.168.1.1/24
*> save
```

Show eth1 Configuration

To show the current eth1 configuration, enter the following command:

```
> show interface ip eth1
```

The display is similar to the following:

```
"eth1" info:

    Interface            eth1
    Flags               (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP MULTICAST>
    IP Address/Mask      192.168.1.1/255.255.255.0
    MTU                  1500
    DHCP                 off
    MAC Address          00:15:93:FE:00:CD
    Speed                N/A
```

ARL Configuration

Address Resolution Logic (ARL) maps Media Access Control (MAC) addresses to specific LAN ports. This enables the switching of packets between ports based on the MAC address in the packet. ARL provides the following features:

- **Dynamic Entries**

  A MAC address learning process automatically builds the ARL table as a forwarding database. The entries the table creates are dynamic entries: entries that are flushed regularly from the table.

  Note: The default aging interval for dynamic ARL entries is 304 seconds; you can change the default by using the **age** *parameter.*

- **Static Entries**

  You can add entries to the ARL table. The entries you create are static entries; static entries are not aged out of the table. Static entries remain in the table until you explicitly delete the entry or you flush the table.

- **Prioritizing Traffic by MAC Address**

  By defining static ARL entries, you can prioritize traffic by the MAC address in the packet. You can assign each static entry to a priority queue. Packets that match the entry are assigned to the specified priority queue. Four priority queues are available: LOWESTQ, LOWQ, HIGHQ, and HIGHESTQ.

  IMPORTANT: Received packets that match a static ARL entry use the priority setting of that entry. This setting overrides all other layer 2 QoS settings for the port (including ToS and 802.1p). You cannot disable this feature.

ARL Configuration Command

To configure a static ARL entry or change a dynamic ARL entry, enter the following command:

```
> config switch arl
```

Table 28 describes the ARL parameters.

Table 28. ARL Parameters

Parameter	Description
index	Index. This is a system-generated entry count.
entrystate	Type of ARL entry (**Dynamic** | **Static**). No default exists.
mac	MAC address. No default exists.
age	Aging interval (in seconds) that determines when dynamic entries are flushed from the table (**16** to **4080**). The value is rounded to the next multiple of 16. The default aging interval is **304** seconds.

Table 28. ARL Parameters

Parameter	Description
priority	Priority assigned to packets that match this entry (**LOWESTQ** | **LOWQ** | **HIGHQ** | **HIGHESTQ**). This parameter applies only to static entries. No default exists. This priority assignment overrides any priority queue assignment by layer 2 QoS.
ports	LAN ports associated with this MAC address (**0**[MII] to 4). No default exists.

Add Static Entry Example

The following example adds a static ARL entry to the forwarding database. The table entry maps a MAC address to port three and assigns its traffic to the highest priority queue:

Index: 2
State: static
MAC address: 00:80:2E:11:11:11
Priority: HIGHESTQ
Port: 3

```
> config switch arl index 2 entrystate static mac
00:80:2E:11:11:11 priority highestq port 3
*> save
```

Change Aging Time Example

The following example increases the aging interval for the ARL table to **320** seconds:

```
> config switch arl age 320
*> save
```

Show ARL Table

To show the current ARL table, enter the following command:

```
> show switch arl

ARL Table

Aging Time: 320

Index State      Mac                Priority     Port
-------------------------------------------------------
1     Static     00:80:2E:34:27:83  LOWQ         MII
2     Static     00:80:2E:11:11:11  HIGHESTQ     3
3     Dynamic    00:E0:4C:00:31:50  N/A          1
4     Dynamic    00:D0:B7:67:07:D8  N/A          1
```

Remove an ARL Entry

To remove an entry from the ARL table, specify its index on the **del switch arl** command.

NOTE: The **del switch arl** *command cannot delete the static entry that maps port* **0** *to the MAC address for the eth1 interface.*

For example, these commands remove the entry with index **2** from the ARL table:

```
> del switch arl index 2
*> save
```

Flush ARL Table

It can be necessary to rebuild the ARL table. To do so, you must flush (empty) the existing ARL table first. Three options are available: flushing all entries, flushing all dynamic entries, or flushing all static entries.

To flush all entries, enter:

```
> clear switch arl
```

To flush all dynamic entries, enter:

```
> clear switch arl state dynamic
```

To flush all static entries, enter:

```
> clear switch arl state static
```

NOTE: The flush is performed when the command is entered. No save command is required.

Layer 2 QoS

The LAN switch in the BSGX4e unit provides a layer 2 Quality of Service (QoS) feature. This feature enables prioritization of network traffic, which is essential for the protection of time-sensitive traffic, such as VoIP phone calls.

Because the BSGX4e device has multiple LAN ports to send traffic to the WAN and only one WAN interface to send that traffic, the device must prioritize the traffic it routes. Layer 2 QoS is provided to guarantee that higher priority traffic is routed while lower priority traffic can be delayed or discarded.

Layer 2 QoS is most effective for traffic switched from the LAN to the IP host.

For a full QoS solution to manage LAN to WAN traffic, layer 3 QoS is also recommended. For information about the layer 3 QoS implementation (called Guarantee of Service, or GoS™), see “GoS Configuration” (page 181).

Priority Queues

Layer 2 QoS provides four queues to classify and prioritize network traffic: LOWESTQ, LOWQ, HIGHQ, and HIGHESTQ. LOWESTQ is the lowest priority queue; HIGHESTQ is the highest priority queue. The four queues are assigned weights (8:4:2:1) that determine the time and number of packets serviced from the queue. The queue weighting cannot be changed.

Scheduling Methods

Two scheduling methods are available:

- **Weighted Fair Queuing (WFQ)**
  All queues are serviced depending on the weight assigned to the queue. No starvation occurs, so that even the lowest priority queue eventually receives service.
- **Fixed**
  All priority packets are serviced from a queue until that queue is empty, and then the next lower-priority queue is serviced, and so on. Starvation can occur: the traffic load for a higher-priority queue can prevent lower-priority queues from being serviced.

Packet Classification

Packets are classified and then assigned to one of the four priority queues. Layer 2 QoS can classify traffic by using any one of the following packet values:

- **Port number**
- **IEEE 802.1p tag**
- **DiffServ/ToS tag**

NOTE: Layer 2 QoS cannot operate if flow control is enabled on any LAN port. To see the current LAN port configuration, enter the command **show switch port**.

Table 29 lists the default priority queues depending on the packet value used for classification.

Table 29. Default Priority Queues

Priority Queue	Port Number	IEEE 802.1p Tag	ToS/DiffServ Tag
LOWESTQ	All ports	1, 2	0 - 15
LOWQ		0, 3	16 - 31
HIGHQ		4, 5	32 - 47
HIGHESTQ		6, 7	48 - 63

Selecting Layer 2 QoS Settings

To select a layer 2 QoS type setting, enter the following command:

```
> config switch qos setting
```

Table 30 describes the parameters for **config switch qos setting**.

Table 30. Layer 2 QoS Setting Parameters

Parameter	Description
type	Packet value that layer 2 QoS uses to classify traffic (**port** | **TOSDiff** | **8021p**). The initial setting is **port**.
scheduling	Method of QoS scheduling to use (**wfq** for Weighted Fair Queueing or **fixed** for fixed scheduling). The default is **wfq**.

Mapping Port Numbers to Priority Queues

The initial setting for layer 2 QoS maps packets to priority queues based on the port number. Initially, all port numbers are mapped to the lowest priority queue (LOWESTQ). Use the following command to map port numbers to the higher-priority queues:

```
> config switch qos port
```

Table 31 describes the parameters for **config switch qos port**.

Table 31. Layer 2 QoS Port Mapping Parameters

Parameter	Description
[**port**]	Port number range to map to the priority queue (**1** to **4**).
priority	Priority queue (**LOWESTQ** | **LOWQ** | **HIGHQ** | **HIGHESTQ**).

Mapping IEEE 802.1p Tags to Priority Queues

If **8021p** is selected as the layer 2 QoS type, use the following command to map tag values to priority queues:

```
> config switch qos ieee
```

For the default mapping of tag values to priority queues, see Table 29.

Table 32 describes the parameters for **config switch qos ieee**.

Table 32. Layer 2 QoS 802.1p Tag Mapping Parameters

Parameter	Description
[**ieee**]	Range of IEEE 802.1p tag values (**0** to **7**).
priority	Priority queue (**LOWESTQ** | **LOWQ** | **HIGHQ** | **HIGHESTQ**).

IEEE 802.1p Tag Mapping Example

The following example selects IEEE 802.1p tag mapping and then maps tags 4 and 5 to the highest-priority queue:

```
> config switch qos setting type 8021p
*> config switch qos ieee 4-5 priority highestq
*> save
```

Mapping ToS/DiffServ Tags to Priority Queues

If **TOSDiff** is selected as the layer 2 QoS type, use the following command to map tag values to priority queues:

```
> config switch qos tos
```

For the default mapping of tag values to priority queues, see Table 29.

Table 33 describes the parameters for `config switch qos tos`.

Table 33. Layer 2 QoS DiffServ/ToS Mapping Parameters

Parameter	Description
[**TOS**]	Range of ToS/DiffServ tag values (**0** to **63**).
priority	Priority queue (**LOWESTQ** | **LOWQ** | **HIGHQ** | **HIGHESTQ**).

Layer 2 QoS Configuration Example

The following example selects port numbers as the layer 2 QoS classification type and then maps port numbers to queues. (Port 1 remains mapped to the default LOWESTQ.)

```
> config switch qos setting type port
*> config switch qos port 2 priority lowq
*> config switch qos port 3-4 priority highestq
*> save
```

Show Layer 2 QoS Configuration

To see the layer 2 QoS classification type, enter the following command:

```
> show switch qos setting

Switch QoS:

Type Scheduling
-------------------------------
Port WFQ
```

To see the mapping of values to priority queues, specify the classification type (**port, 8021p**, or **tos**) on the **show switch qos** command. For example, the following command specifies **port**:

```
> show switch qos port
```

```
Switch QoS:

Port  Priority
-----------------------------------------------
0-1   LOWESTQ
0-2   LOWQ
0-3   HIGHESTQ
0-4   HIGHESTQ
```

7

VLAN CONFIGURATION

This chapter describes how to configure virtual LANs (VLANs) for the BSGX4e device.

NOTE: VLAN configuration is optional. Initially, no VLANs or virtual interfaces (vifs) are configured.

A virtual LAN (VLAN) is a logically independent network, a logical subcomponent of a physical network. Each VLAN functions as a separate network, and so its traffic is isolated from traffic on other VLANs and traffic on the rest of the physical network. This separation can offer protection from Internet multicasts and broadcasts.

The BSGX4e device supports IEEE 801.Q VLAN, which allows up to 64 VLANs on the switch and up to 16 virtual interfaces (vif) in the IP stack. VLANs are integrated into the host IP stack as separate layer 2 Ethernet interfaces.

Complete VLAN configuration requires the following steps:

1. **Assignment of one or more switching ports to the VLAN.**

   A port can be assigned to more than one VLAN. After ports are assigned as members of a VLAN, the LAN switch can forward Ethernet traffic between the ports based on Ethernet addressing. The WAN port can also be assigned to a VLAN.

2. **Creation of a virtual interface for the VLAN.**

   If the VLAN is to communicate beyond the switch, it must have an IP address, and for that, it must have a virtual interface (vif). Up to 16 virtual interfaces can be defined in the IP stack; the virtual interfaces are referenced as vif0 through vif15. A virtual interface can be defined on the LAN or WAN interfaces.

3. **Assignment of an IP address range to the virtual interface.**

4. **Definition of one or more firewall security policies so that the firewall can allow traffic through the virtual interface.**

Assigning Ports to a VLAN

The first step in the configuration of a VLAN is to assign ports as members of the VLAN. The same port can be assigned to more than one VLAN. The ports can be the WAN port or any of the LAN switch ports. Switching is confined to the members of VLANs.

Packet Tagging

Packets can be tagged with the VLAN ID to enable switching on the VLAN. A port is configured as tagged or untagged when it is assigned to the VLAN. VLANs handle packets as follows:

- Untagged ports transmit untagged packets.
- Tagged ports transmit tagged packets.
- Untagged packets delivered to an untagged port are internally tagged with the VLAN ID to which the port belongs; this enables those packets to be switched.
- Untagged packets that arrive at a tagged port are discarded; it is undetermined to which port to assign untagged packets.
- Tagged packets that arrive at a port, other than the VLAN port identified by the VLAN ID in the packets, are dropped.
- IEEE 802.1p packets are considered untagged packets.
- If a port is to be assigned to more than one VLAN, it must be configured as tagged.
- The WAN port must always be configured as tagged.

VLAN Port Assignment Command

To assign ports to a VLAN, enter the following command:

```
> config switch vlan
```

Table 34 describes the parameters for **config switch vlan**.

Table 34. VLAN Configuration Parameters

Parameter	Description
[**vid**]	VLAN identification number (**1** - **4094**).
name	Name or description of the VLAN. It can be up to 32 alphanumeric characters.
wan	VLAN state of the WAN port (**T** = tagged). The WAN port must always be configured as tagged.
p*n*, where *n*=1-4	VLAN state of port *n* (***** = not member, **U** = untagged, **T** = tagged).

VLAN Port Assignment Examples

This section provides examples of how to assign ports to VLANs.

Example 1

The following example assigns port 1 to VLAN 3 as an untagged port:

VLAN ID: 3
VLAN name: v3
Untagged port added to this VLAN: port 1

```
> config switch vlan 3 name v3 p1 u
*> save
```

Example 2

The following example assigns port 1 to both VLANs 3 and 4. To be assigned to more than one VLAN, a port must be configured as tagged. Thus, because port 1 is configured as untagged in Example 1, it must be reconfigured as tagged so that you can also assign it to VLAN 4:

VLAN ID number: 4
VLAN name: v4
Port to add to this VLAN: port 1

```
> config switch vlan 3 p1 t
*> config switch vlan 4 name v4 p1 t
*> save
```

Example 3

The following example assigns the WAN port to VLAN 5. (The WAN port must always be configured as tagged.)

VLAN ID number: 5
VLAN name: v5
Port to add to this VLAN: wan

```
> config switch vlan 5 name v5 wan t
*> save
```

Show VLAN Port Assignments

To see the switching ports assigned to VLANs, enter the following command:

```
> show switch vlan

Switch VLAN:
VID   VLAN Name       WAN P1 P2 P3 P4
-------------------------------------
3     v3               *   T  *  *  *
4     v4               *   T  *  *  *
5     v5               T   *  *  *  *
```

The display shows port 1 (P1) assigned to both VLANs 3 and 4 as a tagged (T) port. The WAN port is assigned to VLAN 5 as a tagged (T) port.

Delete VLAN Port Assignment

To delete a VLAN port assignment, specify the VLAN ID on the command **delete switch vlan**.

NOTE: You must delete the security policies and virtual interface for the VLAN before you can delete the port assignment for a VLAN.

For example, to delete the port assignment for VLAN 3, enter:

```
> delete switch vlan 3
*> save
```

To see the remaining port assignments, enter the following command:

```
> show switch vlan

Switch VLAN:

VID   VLAN Name   WAN P1 P2 P3 P4
---------------------------------
4     v4           *   T  *  *  *
5     v5           T   *  *  *  *
```

Configuring a VLAN Interface

This section describes how to configure a virtual interface (vif) for a VLAN and then assign an IP address to the virtual interface. A virtual interface and IP address assignment enables the BSGX4e to route IP traffic to and from the VLAN.

Configuration Constraints

- You must assign one or more ports to the VLAN before a virtual interface is configured for the VLAN.
- Up to sixteen virtual interfaces can be configured. Virtual interfaces are referenced as vif*n*, where *n* is 0 through 15.
- You can configure a virtual interface on either Ethernet interface (eth0 or eth1). You must configure one or more firewall security policies for the virtual interface. For more information about security policies, see "Firewall Security Policies" (page 130).

Virtual Interface Configuration

To configure a virtual interface for a VLAN, enter the following command:

```
> config interface vlan
```

Table 35 describes the parameters for `config interface VLAN.`

Table 35. Virtual Interface Parameters

Parameter	Description
[vid]	VLAN ID (1 — 4094). Specify the vid used when ports are assigned to the VLAN. To list the VIDs, enter **show switch vlan**.

Table 35. Virtual Interface Parameters (continued)

Parameter	Description
interface	Physical Ethernet interface on which the virtual interface is configured (**eth0** for the WAN interface or **eth1** for the LAN interface). (If **eth0** is specified, the WAN port is automatically assigned to the VLAN.) This parameter is required.
status	Enables the virtual interface (**on | off**).
comment	Optional comment describing the VLAN. The comment can include up to 256 characters; if it contains spaces, enclose the string in quotation marks. Special CLI characters (such as ? and <tab>) are not allowed.

Show Virtual Interface

To see the virtual interfaces that are assigned to VLANs, enter the following command:

```
> show interface vlan
Interfaces:

VID   Interface Status VIF        Comment
------------------------------------------------------------
1     eth1      on     vif0
2     eth0      on     vif1
```

The display shows two VLANs. The virtual interface for VLAN 1 is on the LAN Ethernet interface, eth1, and is referenced as vif0. The virtual interface for VLAN 2 is on the WAN Ethernet interface, eth0, and is referenced as vif1.

VLAN IP Address Assignment

To assign an IP address to the virtual interface, enter the following command:

```
> config interface ip vifn
```

Table 36 describes the parameters for **config interface ip vif*n***.

Table 36. IP Address Assignment Parameters

Parameter	Description
ip	IP address and mask assigned to the specified virtual interface vifn. Specify an address range if DHCP is disabled. The subnet for this virtual interface must not overlap the subnet for any other interface.
mtu	Maximum Transmission Unit (MTU) of the interface (in bytes). The default is **1500** bytes.
dhcp	Enables DHCP for the interface (**on** | **off**). The default is **off**.
status	Enables the virtual interface (**up** | **down**). The default is **up**.

Show IP Address Assignment

To see the IP address assignment for a virtual interface, specify the virtual interface on the **show interface ip** command.

For example, the following command shows the virtual interface vif0:

```
> show interface ip vif0

"vif0" info:

   Interface           vif0
   Flags               (A843) < UP BROADCAST RUNNING SIMPLEX
LINKUP MULTICAST >
   IP Address/Mask     192.168.135.1/255.255.255.0
   MTU                 1500
   DHCP                off
   MAC Address         00:19:09:74:00:01
   Speed               N/A
```

Virtual Interface Configuration Examples

This section provides two examples for how to configure virtual interfaces.

Example 1

The following example assumes that one or more switch ports are assigned to VLAN 1. The example configures a virtual interface for VLAN 1 and shows the interface to determine its vif reference (vif0). The example then assigns an IP subnet to the virtual interface.

VLAN ID: 1
IP address: 192.168.135.1
IP mask: 255.255.255.0

```
> config interface vlan 1 interface eth1
*> show interface vlan

Interfaces:

VID   Interface Status VIF        Comment
-------------------------------------------------------------
1     eth1      on     vif0

*> config interface ip vif0 ip 192.168.135.1/24
*> show interface ip vif0

"vif0" info:

   Interface           vif0
   Flags               (A843) < UP BROADCAST RUNNING SIMPLEX
LINKUP MULTICAST >
   IP Address/Mask     192.168.135.1/255.255.255.0
```

```
   MTU                 1500
   DHCP                off
   MAC Address         00:19:09:74:00:01
   Speed               N/A
*> save
```

Example 2

The following example configures VLAN 2 on the WAN interface eth0. It assumes that the WAN port is assigned to VLAN 2.The example configures a virtual interface for VLAN 2 and shows the interface to determine its vif reference (vif1). The example then assigns an IP subnet to the virtual interface:

VLAN ID: 2
IP address: 192.168.136.1
IP mask: 255.255.255.0

```
> config interface vlan 2 interface eth0
*> show interface vlan

Interfaces:

VID   Interface Status VIF        Comment
------------------------------------------------------------
1     eth1      on     vif0
2     eth0      on     vif1
*> config interface ip vif1 ip 192.168.136.1/24
*> show interface ip vif1

"vif1" info:

   Interface           vif1
   Flags               (A843) < UP BROADCAST RUNNING SIMPLEX
LINKUP MULTICAST >
   IP Address/Mask     192.168.136.1/255.255.255.0
   MTU                 1500
   DHCP                off
   MAC Address         00:19:09:74:00:00
   Speed               N/A
*> save
```

Modifying or Deleting a VLAN

You cannot change a VLAN after you configure it, except to:

- Disable and reenable the virtual interface of a VLAN.
  For example, to disable the virtual interface for VLAN 1, enter:
  `> config interface vlan 1 status off`

- Change the IP address subnet that is assigned to the virtual interface.
  For example, to change the IP address subnet for vif0, enter the new subnet:
  > **config interface ip vif0 ip 1.2.3.4/24**

All other changes require that you delete and recreate the VLAN configuration. To remove a VLAN, everything configured for that VLAN (security policies, IP address assignment, virtual interface, and port assignment) must be removed.

Thus, deletion of a VLAN requires these steps:

1. Delete the firewall policies that apply to the virtual interface (**del security policy**).
2. Delete the IP address assignment for the virtual interface (**del interface ip**).
3. Delete the IP address assignment for the virtual interface (**del interface ip**).
4. Delete the virtual interface (**del interface vlan**).
5. Delete the assignment of switching ports to the VLAN (**del switch vlan**).
6. **Save** the changes**.**

NOTE: When a VLAN is deleted, the BSGX4e device cannot communicate with the IP addresses that had been assigned to the VLAN until those addresses are assigned to another interface. New firewall security policies can also be required.

VLAN Deletion Example

The following example deletes VLAN 1.

1. Show the virtual interface for VLAN 1 by using the following command:

```
> show interface vlan
Interfaces:

VID   Interface Status VIF        Comment
------------------------------------------------------------------
1     eth1      on     vif0
```

2. Show the security policies for vif0 by using the following command:

```
> show security policy

Security Policies:
Id Seq From  Source IP       Dest IP          Source Dest  Proto  NAT QoS
      To                                                  Action ToS IPSec
-------------------------------------------------------------------------
1  1   vif0  any             any              any    9000   tcp    0
       eth0                                                 allow  any
```

3. Delete the security policy for vif0 by using the following command:

```
> del security policy 1
```

4. Delete the IP address assignment for vif0 by using the following command:

```
*> del interface ip vif0
```

5. Delete the virtual interface for VLAN 1 by using the following command:

```
*> del interface vlan 1
```

6. Delete the switch port assignment for VLAN 1 by using the following command:

```
*> del switch vlan 1
```

7. Save the deletion by using the following command:

```
*> save
```

8

ROUTING CONFIGURATION

This chapter describes the configuration options for routing in the BSGX4e device, including:

- Adding static entries to the Address Resolution Protocol (ARP) table.
- Adding static routes to the routing table.
- Starting a Routing Information Protocol (RIP) daemon to receive routing information from other RIP routers. The BSGX4e device supports RIP versions 1 and 2.

NOTE: One or more routes can be defined during installation. To see the current state of the routing table, enter the command **show route table***.*

Introduction

The configuration topics in this chapter refer to three separate protocols that each maintain their own data structure. Each protocol is used for a separate purpose:

- The Address Resolution Protocol (ARP) runs over Ethernet. ARP is used to translate between IP addresses and MAC addresses on Ethernet networks. Normally, ARP works automatically. When a network node sends data to an IP address on its segment, that node broadcasts an ARP request to resolve the IP address to an Ethernet MAC address. The entries in the ARP table map IP addresses to MAC addresses.
- The Internet Protocol (IP) operates at a higher level to route IP packets to addresses on the Internet. It automatically records dynamic entries in a routing table to define routes to destination IP addresses. You can also configure static routes. A route indicates the gateway and interface to be used to send packets to a destination address. The BSGX4e refers to routes in its routing table to determine how to direct traffic between its LAN and WAN interfaces.
- The Routing Information Protocol (RIP) uses a routing daemon. RIP is used in the BSGX4e device only if the daemon is explicitly started. The daemon then listens for RIP messages on the WAN interface from other routers on the network. The daemon uses the RIP message information to maintain the routes in the RIP table.

Configuring ARP

This section describes the Address Resolution Protocol (ARP) in the BSGX4e device. ARP is a network layer protocol that automatically maps IP addresses to hardware Media Access Control (MAC) addresses. When a network node sends data to an IP address on its segment, that node broadcasts an ARP request to resolve the IP address to an Ethernet MAC address.

ARP maintains the ARP table in the device. Each entry in the table maps an IP address to a MAC address. The entries can be dynamic or static, as follows:

- A *dynamic* ARP entry is automatically configured and is automatically flushed after a certain period of time.
- A *static* ARP entry is manually configured (using the command **config route arp**) and is only flushed manually (using the command **del route arp**).

NOTE: The ARP table only maps IP addresses within the IP subnetwork assigned to the device. To see the IP address subnet, enter the command **show interface ip eth1**.

ARP Entry Configuration Command

To define an ARP table entry, enter either of the following commands:

```
> arp set <ip address> <mac address>
> config route arp
```

Table 37 describes the parameters for **config route arp.**

Table 37. ARP Route Parameters

Parameter	Description
[**host**]	IP address.
macaddress	MAC address to be mapped to the IP address.

ARP Entry Example

The following example defines a static ARP entry, which is needed when the MAC address of the receiving device cannot be retrieved:

Host: 192.168.134.163
MAC address: 00:11:22:33:44:55

```
> config route arp 192.168.134.163 macaddress
     00:11:22:33:44:55
*> save
```

Show ARP Table

To show the current ARP table, enter the following command:

```
> show route arp
```

```
ARP entries:

Host             MAC                 Type
-------------------------------------------------------------
192.168.134.1    00:30:64:01:9F:FC   Dynamic
192.168.134.160  00:10:B5:D2:78:42   Dynamic
192.168.134.161  00:11:25:AA:32:11   Dynamic
192.168.134.163  00:11:22:33:44:55   Static
192.168.134.216  00:19:09:74:00:00   Dynamic
```

Delete ARP Entry

To remove an entry from the ARP table, enter the IP address of the entry on either of these commands:

```
> arp del <ip address>
> del route arp <ip address>
```

NOTE: Only static ARP entries can be deleted.

To remove the entry for host 192.168.134.22, enter the following command:

```
> del route arp 192.168.134.22
*> save
```

Flush ARP Table

Flushing the ARP table is a means to clear the ARP table, so it can be rebuilt consistently. For example, this action can be required if computers in the network swap IP addresses.

To flush the ARP table, enter the following command:

```
> arp flush
```

NOTE: The flush is performed when the command is entered. No save command is required.

Protecting ARP Traffic

ARP traffic is essential for the maintenance of the ARP table. The creation of dynamic entries in the ARP table is dependent on ARP traffic from the device to the WAN. Therefore, this traffic must be protected from packet loss.

As described in "GoS Configuration" (page 181), higher-bandwidth LAN traffic is in contention for the lower-bandwidth WAN connection. The BSGX4e device manages this contention by using its QoS mechanisms, especially its Guarantee of Service™ (GoS™) feature. The GoS feature can protect traffic streams by the use of quality groups that define how the traffic is to be protected.

Usually, traffic is classified for quality group protection by using the firewall (as described in “Secure Traffic Processing” (page 129)). However, ARP packets do not pass through the firewall. Therefore, a special command is required to assign ARP traffic to a GoS quality group.

To protect ARP traffic sent from the device to the WAN, specify the name of the appropriate GoS quality group on the following command:

```
> config protocol arp qg
```

The quality group assigned to protect ARP traffic should be a group that ensures low packet loss. It should not allow ARP packets to be treated as best effort (BE) traffic. For a complete discussion of GoS quality groups, see “Quality Groups” (page 182).

ARP Traffic Protection Example

The following commands create and display a quality group named **ARP_Protect**, assign the quality group to ARP traffic, and display the ARP quality group setting:

```
> config qos group ARP_Protect qg A3 type policed committed
100000
*> show qos group ARP_Protect
QoS Quality Groups:
Name         Link  QG  Type     Committed Burst    IPToS COS
-------------------------------------------------------------------------------
ARP_Protect  eth0  A3  pol      100000    0        0     no

*> config protocol arp qg ARP_Protect
*> show protocol arp

ARP Quality Group Settings:
QG     ARP_Protect

*> save
```

Configuring Static Routes

This section describes how to add a static IP route to the routing table in the BSGX4e. Each route in the table specifies the following:

- The packets to which the route applies. Each packet contains a destination IP address. If the destination address is within the *destination address range* specified for the route, the route is applied to the packet.

  A *default route* does not specify a destination address range; instead, it applies to any packet to which no other route applies.
- The IP address of the *gateway* to which the route sends a packet.
- The *interface* through which the route sends a packet.

Route Configuration Command

To define a static route, enter the following command:

```
> config route table
```

Table 38 describes the configuration parameters for **config route table**.

Table 38. Route Configuration Parameters

Parameter	Description
[**dest**]	Range of destination IP addresses to which the route applies. To add a default route to the table, specify **default**.
gw	IP address of the gateway. The gateway must be reachable from the BSGX4e device.
if	Optional interface for the route (**none | lo0** | **eth0** | **eth1**). If no interface is specified, the route interface is determined from the gateway address.

You can also add a route using the maintenance command **route**. Its syntax is:

route add destip [**-gw** gatewayip | **-if** interface] [**-nm** netmask]

Static Route Examples

This section provides examples of how to configure static routes.

Example 1

This example adds a default route to send traffic to gateway 66.206.164.193:

```
> config route table default gw 66.206.164.193
*> save
```

Example 2

This example adds a route that sends all packets destined for subnetwork **192.168.134.0/24** to gateway **66.206.164.194**:

```
> config route table 192.168.134.0/24 gw 66.206.164.194
*> save
```

The route from this example is shown as the last route in the **show route table** example. Its interface is determined from the gateway address.

Show Route Table

To show the current routing table, enter the following command:

```
> show route table

Destination      Gateway          Netmask          Interface
-----------------------------------------------------------
0.0.0.0          66.206.164.193   0.0.0.0          eth0
66.206.164.0     66.206.164.1     255.255.255.0    eth0
127.0.0.1        127.0.0.1        255.0.0.0        lo0
192.168.1.0      192.168.1.1      255.255.255.0    eth1
```

```
192.168.134.0     66.206.164.194    255.255.255.0     eth0
```

Notice that the default route is listed first; its destination address range is shown as `0.0.0.0`, netmask `0.0.0.0`.

Delete a Static Route

To remove a static route from the routing table, specify its destination address and subnet mask on the command **del route table**.

For example, to delete the static route for destination 192.168.134.0, netmask 255.255.255.0, enter the following command:

```
> del route table 192.168.134.0/24
```

You can also delete a route by using the maintenance command **route**. Its syntax is:

route del destip [-gw gatewayip | -if interface] [-nm netmask]

Starting the RIP Daemon

This section describes how the unit can enable dynamic routing by using RIP (Routing Information Protocol). The BSGX4e supports RIP versions 1 and 2.

To use RIP in the BSGX4e, you must start the RIP daemon. The daemon then listens for RIP messages on the WAN interface and uses that information to store routes in a table.

RIP Constraints

- For RIP to be effective, all routers in the network must support RIP version 1 or version 2.
- RIP version 2 is recommended. RIP v2 supports RIP v1 capabilities and also provides:
  - *Variable-Length Subnet Masks (VLSMs)*—support for next-hop addresses, which allows route optimization in certain environments.
  - *Multicasting*—multicasting, instead of broadcasting, reduces the load on hosts that do not support routing protocols.
- The BSGX4e unit is installed at the edge of the network and is intended to run NAT. Thus, the BSGX4e only listens to RIP messages on its WAN interface; it does not support RIP on its LAN interface.
- Use of a RIP daemon on the WAN interface can be a security risk.

RIP Daemon Command

To start the RIP Daemon, enter the command:

```
> config rip daemon
```

Table 38 describes the parameters for **`config rip daemon.`**

Table 39. RIP Daemon Parameters

Parameter	Description
started	Indicates whether the RIP daemon is running. The default value is **no**.
version	Version of the RIP protocol to run (**v1** | **v2**). The default value is **v2** (the recommended version 2).

RIP Daemon Example

This example starts the daemon for RIP version 2:

```
> config rip daemon started version v2
*> save
```

Show RIP Status

To show the current status of RIP, enter the following command:

```
> show rip daemon

RIP Info:

   Started     yes
   Version     v2
```

Show RIP Routes

To show the routes learned by RIP, enter the following command:

```
> show rip route

Destination      Gateway          Netmask          Interface
-------------------------------------------------------------
 192.168.22.73    192.168.134.1    0.0.0.0          eth0

 213.244.0.15     192.168.134.1    0.0.0.0          eth0
```

9 SECURITY CONFIGURATION

This chapter describes how to configure the BSGX4e security features, including:

- Firewall security policies
- Network Address Translation/Application Level Gateway (NAT/ALG) (see "NAT/ALG" (page 134))
- Intrusion Detection System (IDS) (see "IDS" (page 140))

You can also configure Virtual Private Networks (VPN) to ensure secure communications through an insecure network (see "VPN Configuration" (page 153)).

Secure Traffic Processing

The initial BSGX4e configuration has its security features enabled, including its firewall, IDS, and NAT/ALG.

NOTE: For a secure system, it is recommended that all security features remain enabled.

These security features process each incoming packet as follows:

1. Incoming packets are sorted by the information in the packet. The information used from layer 2, layer 3, and layer 4 is listed in Table 40.

Table 40. Traffic Classification

Layer 2	Layer 3	Layer 4
From interface	Source IP	Protocol (Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), or Encapsulating Security Payload (ESP))
To interface	Destination IP	Source port
	IP ToS	Destination port

2. The packets are then compared to the firewall security policies. If the packet matches a policy, the policy action determines if the packet is accepted or discarded.

3. If the firewall accepts a packet, then the IDS checks if the packet format is normal (known as a *sanity check*). Abnormally formatted packets are discarded. IDS then checks whether the packet should be considered an attack and, if so, discards it. Otherwise, the packet is delivered to the destination interface.

4. If the packet is identified as valid, information in its header is modified by NAT/ALG to guard private IP information from public entities.

Firewall Security Policies

This section describes how to define firewall security policies to allow desired incoming traffic.

NOTE: Security policies are also used to classify traffic for layer 3 Quality of Service (QoS) treatment (Guarantee of Service, or GoS). For more information about GoS, see "GoS Configuration" (page 181).

Initial Firewall Security Policies

In the initial device configuration, the firewall security policies reject all incoming traffic; only device management is allowed. The initial security policies perform as follows:

- Traffic from WAN to LAN is rejected.
- Web, Telnet, and SSH traffic that terminates at the BSGX4e device is allowed; all other incoming traffic to the device is rejected.

To see the current firewall policies, enter the command:

```
> show security policy
```

Configuration Constraints

- The firewall is always active. It cannot be disabled.
- Security policies cannot be edited. To change a policy, delete the policy and then recreate it with the desired changes.
- You can create up to 100 security policies.

Security Policy Sequence

An incoming packet can match more than one firewall security policy. Its treatment (acceptance or rejection) is determined by the first policy that the packet matches. Therefore, the sequential order of firewall policies is important. In general, the packet should be compared first to more specific policies (those that specify more packet values).

You can specify the sequential position of a policy. To do so, use the **seq** parameter to specify the beginning or end of the sequence or a position within the sequence.

Policy sequence numbers are always evenly spaced. Thus, when a new policy is inserted within the sequence, policy sequence numbers can be reassigned.

1. For example, assume that policies 3 and 5 exist and a new policy is to be inserted between them.
2. The command specifies 4 as the sequence number of the new policy.
3. However, the new policy is created as policy 5, and the existing policies are renumbered as 3 and 7. The new policy sequence (3, 5, 7) allows future policies to be inserted into the sequence.

Security Policy Configuration Command

To create a security policy, enter this command:

```
> config security policy
```

In the command, parameters are specified for two purposes:

- **To specify matching values** that a packet must have for this policy to apply to the packet. These values can include the source and destination interfaces, the source and destination ports, the protocol, and the IPToS tag value. To match, the packet must have all specified values.
- **To specify treatment options** of any packet that matches this policy. These options can be acceptance or rejection by the firewall, or the treatment defined by a NAT policy or a GoS quality group.

Table 41 describes the parameters for **config security policy.**

Table 41. Security Policy Parameters

Parameter	Description
[**index**]	Specify **new** if the new policy is to be at the beginning or end of the policy sequence; otherwise, specify a number to indicate where the policy is to be inserted in the sequence (see the **seq** parameter).
from	Interface where the packet originated (**self** | **eth0** | **eth1 | vif***n* [*n*=**0**-**15**] | **vpn***n* [*n*=**0**-**9**]). Specify **self** for packets originating at the BSGX4e device.
to	Interface to which the packet is destined (**self** | **eth0** | **eth1 | vif***n* [*n*=**0**-**15**] | **vpn***n* [*n*=**0**-**9**]). Specify **self** for packets destined for the BSGX4e device.
sip	Source IP address or range of IP addresses.
dip	Destination IP address or range of IP addresses.
sport	Source port number or range of port numbers.
dport	Destination port number or range of port numbers.
proto	Protocol specified in the packet (**udp** | **tcp** | **icmp** | **any**).
nat	ID of the NAT policy to be referenced. (Optional; used only for IP addresses or port translation; see "NAT/ALG" (page 134)).

Table 41. Security Policy Parameters (continued)

Parameter	Description
qosqg	Name of GoS quality group. (Not applicable to firewall policies; see "GoS Configuration" (page 181)).
iptos	IP ToS tag value (decimal byte). Specify **any** to match all tag values.
seq	Position of the new policy within the policy sequence (**Begin** | **End** | **Position**). If **Position** is specified, the **index** number specifies where the policy is inserted in the sequence. (See "Security Policy Sequence" (page 130)).
action	Indicates whether a packet matching the policy is accepted or rejected (**allow** | **deny**).

Firewall Security Policy Example

This command configures a security policy that **allows** all TCP traffic from the **eth1** interface, destined for port **9000**, and going out the **eth0** interface**:**

```
> config security policy new from eth1 to eth0 proto tcp dport
9000 action allow
*> save
```

Show Firewall Security Policies

To show the current security policy sequence, enter the following command:

```
> show security policy

Security Policies:
Id Seq From  Source IP        Dest IP          Source Dest  Proto  NAT QoS
       To                                                 Action ToS IPSec
-------------------------------------------------------------------------
1  1   eth1  any              any              any    9000   tcp    0
       eth0                                                allow  any
```

Remove a Firewall Security Policy

To delete a security policy, specify the policy ID on the **del security policy** command. The policy ID is shown in the **show security policy** display.

For example, this command removes security policy 1:

```
> del security policy 1
*> save
```

Show Firewall Log Entries

Packets denied by the firewall are reported in the system log as **Warning** entries.

To protect against Denial of Service attacks, the log records only one packet out of every 64 packets rejected. System logging is described in "Show System Operation Summary" (page 323).

To show the system log, enter the following command:

```
> show logging internal
```

The following log entry is an example that shows the rejection of a packet by the firewall. The entry shows the source, destination, and protocol of the packet.

```
(W)15:28:03: Firewall denied [Id:0] [Src:192.168.134.71:137]
[Dst:192.168.134.255:137] [Proto:UDP] [If: 0]
```

Connection Time-outs

The firewall dynamically opens and closes ports for data traffic. Some TCP-based applications (such as Telnet, FTP, and HTTP) open connections to external servers, which could be left idle for extended periods. Leaving a port open and idle can create a security risk.

Connection timeouts limit how long a port can remain idle before it is closed. You can configure separate timeouts for TCP connections and HTTP connections.

Connection Timeout Command

To configure a connection timeout, enter this command:

```
> config connection tcp
```

Table 42 describes the parameters for **config connection tcp**.

Table 42. Connection Configuration Parameters

Parameter	Description
defaulttimeout	Default TCP timeout in seconds (**60** - **172800** [two days]). The default value is **7200** seconds (two hours).
httptimeout	HTTP timeout in seconds (**60** - **172800** [two days]). The default value is **300** seconds (five minutes).

Show Timeout Settings

To show the current idle timeouts, enter the following command:

```
> show connection tcp

Tcp Connection:

Default Timeout     7200
Http Timeout        300
```

NAT/ALG

Network Address Translation (NAT) provides security by hiding the internal addresses of the private network from the Internet: addresses and/or ports are translated from private IP addresses to public IP addresses, and vice versa.

The BSGX4e device can do both standard and reverse NAT:

- **Standard NAT** (also known as Network Address Port Translation [NAPT])
  Standard NAT translates the source IP address of the LAN to the public WAN IP address. It also changes the source port (for UDP and TCP protocols) or the ICMP identifier. These translations allow several LAN devices to be connected to the WAN through one public IP address.
- **Reverse NAT** (also known as Redirection)
  Reverse NAT forwards traffic and translates addresses between a private IP address and a public IP address. This allows a server in the LAN to be accessed from the Internet (using address forwarding or port forwarding).

The BSGX4e device also supports the Application Layer Gateway (ALG). The ALG enables the transfer of FTP or TFTP traffic through firewall policies and NAT. This is done by creating dynamic holes in the firewall policy and changing IP addresses in application protocol headers. To enable ALG, see "ALG Configuration" (page 140).

Configuring NAT

The NAT policy types on the BSGX4e allow for the following configuration:

- **Static NAT** (also known as inbound mapping)
  One, and only one, public IP address is mapped to one private IP address. Static NAT supports strict translation: only one device on the private network can be recognized through the public IP address on the Internet.
- **NAT address forwarding** forwards a flow from the WAN side that is directed to a public address; it changes the destination IP address to a matching LAN address.
- **NAT port forwarding** forwards the flow from the WAN side that is directed to a specific public IP address and port, changing the destination IP address and port to the configured destination IP address and port of the LAN device. NAT port forwarding supports *NAT overload*. Use of multiple ports enables one public IP address to serve multiple hosts on the private network.

To use NAT, the following configuration steps are required:

1. Verify that NAT is enabled on the WAN interface. (It is initially enabled on eth0.)
2. Configure NAT public addresses and policies as needed for each address and port translation.
3. Configure firewall security policies that reference the NAT policies (see "Security Policy Configuration Command" (page 131)).

For specific steps and examples, see "Port Forwarding" (page 137), "Address Forwarding" (page 138), and "Static NAT Forwarding" (page 138).

Enable NAT on the WAN Interface

NOTE: NAT is initially enabled on the WAN interface (eth0). To verify that it is enabled, enter the command **show security nat interface**.

To enable NAT on a WAN interface, enter the following command:

```
> config security nat interface
```

NOTE: An IP address must be assigned to the WAN interface (see "WAN Interface Configuration" (page 91)).

You can also enable NAT for virtual interfaces (**vif**) and VPN interfaces (**vpn**) defined on the physical WAN interface. For more information about vif interfaces, see "VLAN Configuration" (page 111). For more information about vpn interfaces, see "VPN Configuration" (page 153).

Table 43 describes the parameters for **config security nat interface.**

Table 43. NAT Status Parameters

Parameter	Description
[**interface**]	WAN interface (**eth0** | **vif***n* [*n*=**0**-**15**] | **vpn***n* [*n*=**0**-**9**]).
status	Indicates whether NAT is enabled or disabled for the interface.

Enable NAT Interface Example

The following command enables NAT on the WAN interface, **eth0**:

```
> config security nat interface eth0 status on
*> save
```

Show NAT Interface Status

To view the current NAT interface status, enter the following command:

```
> show security nat interface

Interfaces:

Interface Status Alias
-----------------------------------------
eth0      on     192.168.134.217
```

The display also shows the IP address (Alias) currently assigned to the **eth0** interface.

Configuring NAT Policies

When translating addresses, NAT references policies that map addresses and ports. These policies enable static NAT, port forwarding, and address forwarding.

NOTE: You must enable NAT on the WAN interface.

To configure a NAT policy, enter the following command:

```
> config security nat policy
```

Table 44 describes the parameters for **config security nat policy.**

Table 44. NAT Policy Configuration Parameters

Parameter	Description
[id]	Policy ID number. Specify **new** when creating a new policy.
type	Type of policy (**static** | **rport** | **raddr**). Specify **rport** for port forwarding; **raddr** for address forwarding.
address	IP address to be translated (a public address for a static NAT policy; a private address for a redirect NAT policy). A public address must have been specified on a **config security nat public** command.
port	Port to be translated (public for a static NAT policy; private for a redirect NAT policy). This parameter is required for **rport** policies (port forwarding).

Examples of NAT policies are shown in "Port Forwarding" (page 137), "Address Forwarding" (page 138), and "Static NAT Forwarding" (page 138).

Configuring NAT Public Addresses

For static NAT, you must configure the public IP address. This section describes how to add public IP addresses to NAT.

NOTE: NAT must be enabled on the WAN interface.To see the NAT interface status, enter **show security nat interface.**

To configure a public address, specify the IP address on the following command:

```
> config security nat public
```

For example, the following command defines the public IP address **192.168.134.199**:

```
> config security nat public 192.168.134.199
*> save
```

To see the configured public addresses, enter the following command:

```
> show security nat public

Addresses:

Address
-------------------------------------------------------
```

```
192.168.134.199
```

Port Forwarding

NAT port forwarding requires the following policies:

- A NAT policy of type *redirect port* (**rport)** that provides the private information.
- A security policy that provides the public information and references the NAT policy (see "Security Policy Configuration Command" (page 131)).

NOTE: NAT must be enabled on the WAN interface. To see the NAT interface status, enter **show security nat interface***.*

Port Forwarding Example 1

For example, the following commands enable address translation for a Web server on the LAN:

1. Define a NAT policy of type redirect port (rport).

It provides the private LAN address and port (**10.0.1.101:80**) of the Web server:

```
> config security nat policy new type rport address
10.0.1.101 port 80
```

The new NAT policy is assigned index **1**.

2. Define the security policy.

It provides the public information: **TCP** traffic sent from **eth0** to port **12999** of the BSGX4e unit (**self**) is forwarded according to NAT policy **1**:

```
*> config security policy new from eth0 to self dport 12999
proto tcp nat 1
```

3. Save the configuration. Enter the following command:

```
*> save
```

Port Forwarding Example 2

This example configures the unit to forward traffic that arrives on UDP port 9000 to LAN IP address 10.0.1.130, destination port 2600.

1. Define a NAT policy of type redirect port (rport).

It provides the private LAN address and port (**10.0.1.130:2600**):

```
> config security nat policy new type rport address
10.0.1.130 port 2600
```

The new NAT policy is assigned index **2**.

2. Define the security policy.

It provides the public information: **UDP** traffic sent from **eth0** to port **9000** of the BSGX4e unit (**self**) is forwarded according to NAT policy **2:**

```
*> config security policy new from eth0 to self dport 9000
proto udp nat 2
```

3. **Save the configuration.** Enter the following command:

```
*> save
```

Address Forwarding

NAT address forwarding requires the following configuration:

- A NAT policy of type *redirect address* (**raddr**) that provides the private information.
- A security policy that provides the public information and references the NAT policy (see "Security Policy Configuration Command" (page 131)).

NOTE: NAT must be enabled on the WAN interface. To see the NAT interface status, enter **show security nat interface**.

Address Forwarding Example

This example configures NAT to translate a public IP address to a private LAN IP address.

1. **Define a raddr NAT policy** to provide the private LAN address (**10.0.1.102**):

```
> config security nat policy new type raddr address
10.0.1.102
```

   The new NAT policy is assigned index **3**.

2. **Define the security policy** to provide the public information.

   WAN (**eth0**) traffic sent to the unit using IP address **192.168.134.210** is forwarded according to NAT policy **3**.

```
*> config security policy new from eth0 to self dip
192.168.134.210 nat 3
```

3. **Save the configuration.** Enter the following command:

```
*> save
```

Static NAT Forwarding

Static NAT forwarding requires the following configuration:

- a NAT public address
- a NAT policy of type **static** that defines the public information
- a security policy that defines the private information (see "Security Policy Configuration Command" (page 131))

NOTE: NAT must be enabled on the WAN interface. To see the NAT interface status, enter **show security nat interface**.

For example, the following commands enable translation of a private LAN address to a public IP address.

1. **Define the public address as a NAT address** (192.168.134.65):

   > **config security nat public 192.168.134.65**

2. **Define a static NAT policy** to provide the public IP address (192.168.134.65):

   *> **config security nat policy new type static address 192.168.134.65**

   The new NAT policy is assigned index **4**.

3. **Define a security policy** to provide the private information.

   LAN (**eth1**) traffic from IP address **10.0.1.103** is forwarded to the WAN (**eth0**) according to NAT policy **4**:

   *> **config security policy new from eth1 to eth0 sip 10.0.1.103 nat 4**

4. **Save the configuration.** Enter the following command:

   *> **save**

Show NAT Policies

To list the NAT policies and then the security policies, enter the following commands:

```
> show security nat policy

Policies:

Id Type   Address          Port
-------------------------------------------------
1  rport  10.0.1.101       80
2  rport  10.0.1.130       2600
3  raddr  10.0.1.102       0
4  static 192.168.134.65   0

> show security policy

Security Policies:

Id Seq From  Source IP       Dest IP         Source Dest  Proto  NAT
Qos    To                                                 Action ToS
-------------------------------------------------------------------------
5  7   eth0  any             any             any    12999 tcp    1
       self                                               allow  any
6  9   eth0  any             any             any    9000  udp    2
       self                                               allow  any
7 11   eth0  any             192.168.134.199 any    any   any    3
       self                                               allow  any
8 13   eth1  10.0.1.103       any             any    any   any    4
       eth0                                               allow  any
```

Notice that the NAT field in the security policy list references the Id of a NAT policy.

ALG Configuration

The Application Layer Gateway (ALG) enables the transfer of FTP and TFTP traffic through firewall policies and NAT. This is done by creating dynamic holes in the firewall policy and changing IP addresses in application protocol headers.

ALG is supported only for FTP and TFTP protocols.

NOTE: NAT must be enabled on the WAN interface. (See "Enable NAT on the WAN Interface" (page 135)).

Configuration Command

To specify the applications for which ALG is enabled (FTP and/or TFTP), enter the following command:

```
> config security alg
```

Table 45 describes the parameters for **config security alg**.

Table 45. ALG Configuration Parameters

Parameter	Description
ftp	Indicates whether ALG is enabled for FTP traffic (**yes** | **no**).
tftp	Indicates whether ALG is enabled for TFTP traffic (**yes** | **no**).

Enable ALG Example

The following command enables ALG for FTP traffic:

```
> config security alg ftp yes
*> save
```

Show ALG

To show the current ALG configuration, enter the following command:

```
> show security alg

ALG Settings:

Name     Active
------------------
FTP      yes
TFTP     yes
```

IDS

The Intrusion Detection Service (IDS) defense is designed to protect against attacks that are destined for the BSGX4e device or the LAN network.

This section describes the attack types against which IDS provides protection. In the initial configuration of the unit, IDS protection is enabled against all attack types.

NOTE: For a secure system, it is recommended that IDS protection remain enabled. To check that specific protections are enabled, enter the following commands:

- **show ids anomaly**
- **show ids flood activity**
- **show ids scan**
- **show ids spoof**

NOTE: To protect itself from being overwhelmed by a denial of service attack, the IDS counter is limited to reporting 64 packets per second. Thus, the actual packet rate may be greater than the value reported by the IDS counter.

Attack Types

IDS inspects all inbound and outbound network activity and identifies patterns that can indicate system attacks. Table 46 lists the applicable protocols.

IDS identifies the following types of attacks:

- **Packet anomaly**
  Protects the unit from abnormal packets that intend to crash the destination.
- **Firewall**
- **Scan**
  Protects the unit from useless packets that intend to locate “holes” in the firewall.
- **Flood**
  Protects the unit from excess incoming packets that would overload the unit.
- **Spoof**
  Protects the LAN network and the unit from intrusion. IDS spoof protection is available for all configured interfaces.

Table 46. Protocols to which IDS Attack Protection Applies

Attack	TCP	UDP	ICMP	RTP	IP	ARP		
Anomaly	X		X	X	X			
Flood	X	X	X			X		
Scan	X	X	X					

Packet Anomaly Protection

This section describes the packet anomalies for which IDS provides protection.

Protection for two packet anomalies can be enabled or disabled. The two anomalies are:

- IP fragment is overlapped (`fragoverlap`).
- Too many fragments need to be reassembled (`fragoverrun`).

Protection against all other anomalies is enabled by default and cannot be disabled. Table 47 lists the other anomalies.

Table 47. Packet Anomaly Attacks

IP	ICMP	TCP	RTP
Version	Length	Header fragmentation	SSRC ID
TTL (Time to Live)		Flags	
Checksum			
Length			
Options			

Fragment Anomaly Activation

Packet fragments are often used to evade detection when attacking a system. The packet fragment anomalies are:

- **fragoverlap**
  The offset of one fragment overlaps the offset of another fragment. For example, if the offset of the first fragment is 0 and its length is 800, the offset of the second fragment should be 800. If it is less than 800, the second fragment overlaps the first fragment. This condition can indicate an attack.
- **fragoverrun**
  Triggers when a reassembled fragmented datagram exceeds the declared IP data length or the maximum datagram length. By definition, no IP datagram can be larger than 65,535 bytes; systems that try to process these large datagrams can crash. This type of fragmented traffic can indicate a denial of service attempt.

To enable or disable protection against packet fragment anomalies, enter the following command:

```
> config ids anomaly
```

Table 48 describes the parameters of **`config ids anomaly`**.

Table 48. Packet Fragment Anomaly Parameters

Parameter	Description
`[attack]`	Attack type to detect (**fragoverlap** | **fragoverrun**)

Table 48. Packet Fragment Anomaly Parameters (continued)

Parameter	Description
active	Indicates whether to activate this attack detection.

Example Activating Fragment Anomaly Protection

These commands activate IDS protection for fragment anomalies:

```
> config ids anomaly fragoverlap active yes
*> config ids anomaly fragoverrun active yes
*> save
```

Show Fragment Anomaly Activation

To see the status of IDS protection against fragment anomalies, enter the following command:

```
> show ids anomaly

IDS IP Anomaly:

Attack                    Active
-----------------------------------------------------------
fragoverlap               yes
fragoverrun               yes
```

Flood Protection

This section describes IDS flood detection. In general, flood attacks result in denial of service. IDS can detect floods targeted at protocols and services.

IDS refers to a threshold value to detect a flood attack. The threshold varies depending on the protocol or service being protected. Some threshold values are listed in the display for the command **show ids flood activity**; service thresholds are discussed in "Setting Flood Thresholds" (page 145).

IDS Flood Types

You can change IDS flood detection for the following flood activity types:

- **udpflood**
  In a UDP flood, UDP packets are sent to inactive services (ports); the receiver then replies with an ICMP Destination Unreachable packet. The flood results in Denial-of-Service, due to sending out several ICMP packets.
- **icmpflood**
  An ICMP flood sends over-sized or an excessive number of ICMP packets. This situation can crash the TCP/IP stack, causing the unit to stop responding to TCP/IP requests.
- **arpflood**

In an ARP flood, an unauthorized attempt is made to change the ARP table, which can result in Denial of Service or Man-in-the-Middle attacks. Also, repeated packets can be sent, resulting in multiple MAC addresses being saved in the ARP tables, which causes packets to be broadcast, rather than sent to one destination.

- **synflood**
  SYN (synchronization) packets are repeatedly sent to every port on the server, using fake IP addresses. SYN flooding can result in denial of service.
- **espflood**
  Encapsulated Security Payload (ESP) flood. An ESP flood sends bad IPsec traffic. Packets are discarded after the threshold rate limit is reached. The default threshold is 100 packets/second.
- **unknowipprotoflood**
  This flood activity type refers to floods for IP protocols other than those listed specifically.
- **cdpflood**
  Cisco Discovery Protocol (CDP) flood. A CDP flood sends CDP packets at a high rate. Packets are discarded after a threshold rate limit is reached.
- **unknowntypeflood**
  This flood activity type refers to floods targeting Ethernet activities, such as ARP, IP, and PPPoE.

Flood Detection Activation

To activate detection of a flood type, enter the flood type on the following command:

```
> config ids flood activity
```

Table 49 describes the parameters for **config ids flood activity**.

Table 49. Flood Detection Activation Parameters

Parameter	Description
[**attack**]	Flood type to detect (**udpflood** | **icmpflood** | **arpflood** | **synflood** | **espflood** | **unknowipprotoflood** | **cdpflood** | **unknowntypeflood**).
active	Indicates whether this detection is activated.

Example of Flood Detection Activation

The following command activates IDS detection of ICMP floods:

```
> config ids flood activity icmpflood active yes
*> save
```

Show Flood Detection Activation

To see the status of IDS protection against floods, enter the following command:

```
> show ids flood activity

IDS Flood:

Attack                Active  Name
-------------------------------------------------------------
udpflood              on      UDP Flood
icmpflood             on      ICMP Flood (Threshold = 100 pp*
arpflood              on      ARP Flood (Threshold = 255 pps)
synflood              on      SYN Flood (Threshold = 50 pps)
espflood              on     ESP Flood
unknowipprotoflood    on      Unknown IP proto Flood
cdpflood              on      CDP Flood (Threshold = 50 pps)
unknowntypeflood      on      Unknown Ethernet Type Flood
```

Setting Flood Thresholds

This section describes how to change threshold values for IDS flood protection.

IDS refers to a threshold value to detect a flood attack. You can change the threshold for some protocols and services:

- known protocols: ARP, ICMP, UDP, TCP, ESP
- any protocol other than the known protocols listed above (`unknown_ip_proto`)
- known services: DHCP, DNS, IKE, MGCP, RADIUS, RIP, SIP, SNMP, SNTP, TFTP
- any service (port) other than the known services listed above (`unknown_port`)

Table 50 lists the default threshold values:

Table 50. Default Flood Threshold Values

Protocol or Service	Default Threshold Level	Protocol or Service	Default Threshold Level	Protocol or Service	Default Threshold Level
dns	20	**radius_2**	100	**tftp**	100
esp	100	**rip**	20	**unknown_IP_proto**	500
ike	100	**sip**	255	**unknown_port**	500
mgcp	255	**snmp**	200		

To change the threshold value for a protocol or service, enter the following command:

```
> config ids flood settings
```

Table 51 describes the parameters for **`config IDS flood settings`**.

Table 51. Flood Threshold Setting Parameters

Parameter	Description
[**service**]	Protocol or service whose threshold value is changed (**dhcp** | **dns** | **esp** | **ike** | **mgcp** | **radius_1** | **radius_2** | **rip** | **sip** | **snmp** | **sntp** | **tftp** | **unknown_IP_proto** | **unknown_port**).
threshold	Threshold level (minimum number of packets/second) to be considered an attack.

To see the current threshold values for IDS flood protection, enter the following command:

```
> show ids flood settings

IDS Flood:

Protocol                  Threshold
-----------------------------------------------------------
dhcp                      10
dns                       20
esp                       100
ike                       100
mgcp                      255
radius_1                  100
radius_2                  100
rip                       20
sip                       255
snmp                      150
sntp                      10
tftp                      100
unknown_IP_proto          500
unknown_port              1000
```

Scan Protection

This section describes IDS scan protection. You can activate IDS scan protection for ICMP, UDP, and TCP SYN messages. A threshold value determines the number of messages sent that constitute an attack.

When IDS detects a scan attack, it bans traffic for that protocol (ICMP, UDP, or TCP) for the timeout interval. You can change the default timeout value.

IDS scan protection can detect the following scan types:

- **udpportscan**
  A port scan is a series of messages sent by a potential system intruder to determine which services the system provides. The services are each associated with a well-known port number. Port scanning suggests where the intruder could probe for weaknesses.

- **tcpsynscan**
  A TCP SYN scan is a series of messages sent with the TCP Syn flag set.
- **pingsweep**
  ICMP requests are sent to multiple hosts. A ping sweep is a means to locate network devices that are active and responding, and so, could be targets for an attack.

IDS Scan Activation

To activate a scan type or change its timeout value, enter the following command:

```
> config ids scan
```

Table 52 describes the configuration parameters for **config ids scan**.

Table 52. IDS Scan Configuration Parameters

Parameter	Description
[attack]	Scan attack type (**udpportscan** | **tcpsynscan** | **pingsweep**).
timeout	Timeout after an attack is detected (in seconds). The default is **50** seconds for **udpportscan** and **tcpsynscan** and **60** seconds for **pingsweep**.
active	Indicates whether detection for the attack type is activated.

IDS Scan Activation Example

The following command activates detection of UDP port scans and sets its timeout value to 30 seconds:

```
> config ids scan udpportscan timeout 30 active yes
*> save
```

Show IDS Scan Status

To see the status of IDS scan protection, enter the following command:

```
> show ids scan
IDS Scan:

Attack          Threshold Timeout Active Name
-------------------------------------------------------
udpportscan     7         50      on     UDP Port Scan
tcpsynscan      7         50      on     TCP SYN Scan
pingsweep       3         60      on     Ping Sweep
```

Spoof Protection

This section describes IDS spoof detection. You can activate IDS spoof detection for all IP interfaces, including eth0, eth1, virtual interfaces (vif*n*), and VPN interfaces (vpn*n*).

By default, IDS assumes the trust settings shown in Table 53.

- IDS assumes that spoof attacks arrive from the WAN, and so, by default, it assigns untrusted status to the eth0 interface (and to virtual WAN interfaces). This activates spoof detection for that interface.
- However, IDS assumes that LAN traffic is safe and the LAN is not a likely source of spoof attacks, and so, by default, spoof protection is not needed on LAN interfaces (eth1 and virtual LAN interfaces).
- IDS assumes that a VPN secures its traffic from spoof attacks. Thus, by default, it assigns trusted status to vpn*n* interfaces.

Table 53. Default Trust Settings for Interfaces

Interface	Trust Setting
eth0	untrusted
eth1	trusted
WAN vif*n*	untrusted
LAN vif*n*	trusted
vpn*n*	trusted

IDS Spoof Command

To change IDS spoof detection on an IP interface, enter the following command:

```
> config ids spoof
```

Table 54 describes the parameters for **config ids spoof.**

Table 54. IDS Spoof Configuration Parameters

Parameter	Description
[**name**]	IP interface to be protected (**eth0** | **eth1** | **vif*n***, where *n*=0-15 | **vpn*n***, where *n*=0-9).
type	Indicates whether the interface is a trusted or untrusted interface (**trusted** | **untrusted**). IDS checks for spoof attacks on untrusted interfaces only.

IDS Spoof Example

This command activates IDS spoof detection on the eth1 interface by defining its type as untrusted:

```
> config ids spoof eth1 type untrusted
*> save
```

Show IDS Spoof Status

To see the interfaces on which IDS checks for spoof attacks, enter the following command:

```
> show ids spoof
```

In the following example, IDS only checks for spoofs on the WAN interface, eth0.

```
IDS Spoofing:

Interface  Type
-------------------------------------------------------
eth0       untrusted
eth1       trusted
vif0       trusted
vpn0       trusted
```

IDS Statistics

This section shows how to view IDS statistics. IDS keeps a count for each type of attack.

NOTE: To protect itself from being overwhelmed by a denial of service attack, the IDS counter is limited to reporting 64 packets per second. Thus, the actual packet rate can be greater than the value reported by the IDS counter.

To see the IDS attack counts, enter the following command:

```
> show ids attacks

IDS Attacks:

Attack                        Count
-------------------------------------------------------------
PACKET ANOMALY
   Layer 3
Land attack                    0
IP with bad options            0
IP with unsupported options    0
Bad checksum                   0
Bad TTL                        0
Bad IP version                 0
Bad IP length                  0
Source IP is NULL              0
IP fragment too short          0
   Layer 4
TCP no flags set (Null Scan)   0
TCP all flags set              0
TCP flags are nonsense         0
TCP SYN & FIN                  0
TCP SYN with no ACK            0
```

```
TCP FIN with no ACK          0
TCP SYN + IP MF              0
Large ICMP (>1024)           0

FIREWALL
TCP Flags not in connection  0
TCP Orphaned FIN             0
Firewall Policy              0
No route to destination      2
IP fragment is overlapped    0
IP datagram is overrun       0
Too many IP datagram in reassembly state 0
Link table overflow          0

SCAN
TCP SYN scan                 0
UDP Port Scan                0
Ping sweep                   0

FLOOD
  Layer 2/3
ARP Flood                    0
STP flood                    0
CDP flood                    0
Unknown Ethernet Type flood  0
  Layer 4
UDP Flood                    0
UDP Rate limiting to host overflow 0
ICMP flood                   0
SYN Flood                    0
ACK Flood                    0
ESP flood                    0
Unknown IP Proto flood       0

SPOOFING
Spoofing detected            0
Spoofed with Loopback        0

VOICE
Bad SSRC Id                  0
```

Clear IDS Statistics

To clear all counts kept by IDS, enter the following command:

```
> clear ids attacks
```

Show IDS Log Entries

IDS reports attacks as `Warning` entries in the system log. For more information about the system log, see "Show System Operation Summary" (page 323).

NOTE: To avoid filling the log and the resulting denial of service, IDS reports only one attack for every 64 attacks detected.

To see the log entries, enter the following command:

```
> show logging internal
```

The following example shows two IDS entries; the first reports a `Bad IP version` attack, and the second reports a `Ping flood` attack:

```
(W)15:27:59: Defended 'Bad IP version'
[Src:192.168.134.140:128] [Dst:192.168.134.191:128]
[Proto:UDP] [If: 0]
(W)15:28:00: Defended 'Ping flood' [Src:192.168.134.161]
[Dst:192.168.134.217] [Proto:ICMP] [If: 0]
```

10 VPN CONFIGURATION

This chapter describes how to configure Virtual Private Networks (VPN).

VPN Support

A VPN provides a secure connection through an insecure shared network, such as the Internet. The BSGX4e device supports VPNs using the IP security (IPsec) protocol.

An IPsec VPN serves as a point-to-point tunnel interface. For example, a VPN could connect to an Internet Service Provider (ISP). This allows the BSGX4e to send some or all of its WAN traffic across an encrypted tunnel to the ISP gateway, rather than in clear text.

VPN Constraints

VPN support in the BSGX4e device has the following constraints:

- Only tunnel mode is supported.
- Up to 10 tunnels can be set up concurrently.
- IPsec encryption can use 3DES (168) or AES (128, 192, and 256).
- IPsec authentication can use SHA (96) or MD5 (96).
- IPsec uses the Internet Key Exchange (IKE) protocol to set up its security associations (SAs):
  - IKE uses preshared keys. (Certificate Authority (CA) certificates are not supported.)
  - IKE encryption can use DES (56), 3DES (168), AES (128, 192, and 256), or BLOWFISH (128)
  - IKE authentication can use SHA or MD5.
  - The duration of the SA lifetime timer can be configured. When the timer expires, the SA is renegotiated, thus, increasing security.

Security Associations (SAs)

The Internet Key Exchange (IKE) protocol negotiates SAs. SAs determine how data is encrypted, decrypted, and authenticated by the secure gateways. When configured, the BSGX4e device can function as a secure gateway.

SAs are dynamic; each SA is automatically negotiated during the first attempt to send an IP packet between LANs. SAs expire after a finite time, but prior to expiration, a replacement SA is automatically negotiated.

After IPsec SAs are established, the VPN becomes operational; secure gateways use IPsec tunneling to secure IP traffic between LANs. Each IP packet sent between LANs is securely encrypted inside an Encapsulated Security Payload (ESP) packet during transmission between the secure gateways.

Two types of SAs exist:

- IKE SA
  Established during IKE main mode negotiations, IKE SAs determine how to secure subsequent IKE negotiations between the secure gateways.
- IPsec SA
  Established during IKE quick mode negotiations, IPsec SAs determine how to secure IP traffic between the LANs.

Configuration Elements

VPN configuration requires the configuration of the following:

- SA lifetimes (IKE and IPsec) and the IPsec DH group (optional; defaults are provided).
- An IKE preshared key record for the remote gateway.
- An IPsec proposal (optional; a default is provided).
- An IPsec policy specifying the IP addresses and the IPsec proposal.
- An IP address for the tunnel interface.
- A route for tunnel traffic.
- Security policies to allow:
  - IKE and ESP traffic through the firewall.
  - Tunnel traffic through the firewall.
  - NAT (address translation) for tunnel traffic (optional).

For a VPN configuration example, see “VPN Configuration Examples” (page 163).

IKE

The Internet Key Exchange (IKE) protocol provides utility services for IPSec. It defines how pairs of secure gateways negotiate IKE security associations (IKE SAs). The IKE SAs that the BSGX4e negotiates are determined by the configuration of IKE preshared keys and IKE parameters.

An IKE configuration uses:

- IKE policies (predefined)
- IKE parameter settings (`config ike parameters` on “IKE Lifetime Parameters” (page 155))
- IKE preshared key records (`config ike preshared` on “IKE Preshared Key Records” (page 156))

IKE Policies

An IKE policy is a set of security parameters used when negotiating an IKE SA with a remote secure gateway. Sixteen predefined IKE policies are provided, offering every combination of encryption algorithm, hash digest, and Diffie-Hellman group available. The IKE policies that the BSGX4e can accept or offer are listed in priority order.

NOTE: To negotiate an IKE SA, the remote gateway must have an IKE policy configured to match one of the local predefined IKE policies.

To see the predefined IKE policies, enter the following command:

```
> show ike policies
```

```
IKE Policies:
Priority Encryption Hash Group
-------------------------------------------------------------
1        3DES       SHA  DH1024
2        3DES       SHA  DH768
3        3DES       MD5  DH1024
4        3DES       MD5  DH768
5        AES        SHA  DH1024
6        AES        SHA  DH768
7        AES        MD5  DH1024
8        AES        MD5  DH768
9        DES        SHA  DH1024
10       DES        SHA  DH768
11       DES        MD5  DH1024
12       DES        MD5  DH768
13       BLOWFISH   SHA  DH1024
14       BLOWFISH   SHA  DH768
15       BLOWFISH   MD5  DH1024
16       BLOWFISH   MD5  DH768
```

IKE Lifetime Parameters

You can configure the length of the lifetime of an IKE SA. When the lifetime of an IKE SA expires, the SA is renegotiated. Thus, a shorter lifetime can increase security.

To change IKE parameter values, enter the following command:

```
> config ike parameters
```

Table 55 describes the parameters of **config ike parameters.**

Table 55. IKE Parameters

Parameter	Description
lifetime	Default IKE SA lifetime (in seconds). The initial setting is **86400** (24 hours).

Table 55. IKE Parameters (continued)

Parameter	Description
maxlifetime	Maximum IKE SA lifetime (in seconds). The initial setting is **259200** (72 hours).

Show IKE Parameters

To show the IKE parameter settings, enter the following command:

```
> show ike parameters

IKE Parameters:
   Lifetime            86400 seconds
   Maximum Lifetime    259200 seconds
```

IKE Preshared Key Records

An IKE preshared key record specifies the preshared key used to encrypt Internet Security Association and Key Management Protocol (ISAKMP) messages. An IKE preshared key record defines the key (similar to a password) used to authenticate a remote secure gateway.

IKE Preshared Key Requirements

- Every IKE SA negotiation refers to a preshared key record to get the key value shared with the peer, that is, the remote secure gateway. Usually, each VPN has its own preshared key record. However, you can configure a default key record.
- The same preshared key value must be configured at the remote secure gateway.
- All IKE negotiations run over UDP on port 500; you must configure a security policy to allow UDP traffic with destination port 500 of the remote secure gateway.
- The BSGX4e does not support aggressive mode IKE negotiations; you must configure the remote secure gateway to use main mode. Main mode is the default for most IKE implementations.

IKE Preshared Key Command

To configure an IKE preshared key record, enter the following command:

```
> config ike preshared
```

Table 56 describes the parameters of **config ike preshared**.

Table 56. IKE Preshared Configuration Parameters

Parameter	Description
[**peer**]	IP address of the remote gateway. To define a default key for every peer, specify **0.0.0.0** as the gateway.

Table 56. IKE Preshared Configuration Parameters (continued)

Parameter	Description
key	Preshared key (up to 50 characters). The same preshared key must be configured at the remote gateway.

IKE Preshared Key Record Examples

This example configures an IKE preshared key record:

IP address of remote gateway: `10.0.1.2`
Preshared key:`1J3W5RE89`

```
> config ike preshared 10.0.1.2 key 1J3W5RE89
*> save
```

This example configures a default key:

IP address for default key: `0.0.0.0`
Preshared key:`123456789`

```
> config ike preshared 0.0.0.0 key 123456789
*> save
```

Show IKE Preshared Key Records

To show the current IKE preshared key records, enter the following command:

```
> show ike preshared

IKE Preshared:

Peer            Mode Key
-----------------------------------------------------------
0.0.0.0         main 123456789
10.0.1.2        main 1J3W5RE89
```

The default preshared key is the record listed for peer `0.0.0.0`. If a preshared key record is not defined for a gateway, the default key is used.

Show IKE Security Associations

This command can be used to verify that the expected IKE SAs have been negotiated after a successful main mode negotiation.

The command **show ike sa** displays the IKE SAs currently negotiated with other IKE peers in main mode negotiations; if no negotiation has occurred, no information is displayed.

To show the current IKE SA configuration, enter:

```
> show ike sa
```

After successful negotiation, the display is similar to the following:

```
IKE SAs:

LocalAddr       Group      Encryption Duration InitiatorCookie
RemoteAddr      Initiator  Hash       LifeType ResponderCookie
-------------------------------------------------------------
172.30.3.55     DH1024     3DES       86387    0xE92F945832B6D96B
172.29.3.56     Yes        SHA        Seconds  0xC1FDA432155BF2FE
```

Table 57. **IKE SAs**

Parameter	Description
LocalAddr, RemoteAddr	IP addresses of the two ends of the tunnel.
Initiator	The field reports Yes if the unit initiates the SA negotiation.
Group, Encryption, Hash	Algorithms used to create a secure channel between the two peers for further IPsec SA negotiation.
Duration, LifeType	Remaining lifetime.
InitiatorCookie, ResponderCookie	These cookies are identification values inside the IKE packets sent between the two peers; they can be matched against a packet capture. Use this information to verify system operations or to troubleshoot errors.

Clear IKE SAs

To clear the IKE SAs, enter the following command:

```
> clear ike sa
```

Show IKE Statistics

To see the current IKE statistics, enter the following command:

```
> show protocol ike

IKE Stats:

Packets Sent    0                Packets Received    0
Events Sent     0                Events Received     0
```

IPsec

IPsec provides data confidentiality, data integrity, and data authentication between peers.

The Internet Key Exchange (IKE) protocol defines how pairs of secure gateways negotiate IKE security associations (IPsec SAs). The IPsec SAs negotiated are determined by the configuration of IPsec policies and IPsec proposals.

An IPsec configuration uses:

- IPsec parameter settings (`config ipsec parameters` on "IPsec Parameters" (page 159))
- IPsec proposals (`config ipsec proposal` on "IPsec Proposals" (page 160))
- IPsec policies (`config ipsec policy` on "IPsec Policies" (page 160))

NOTE: IPsec traffic on the BSGX4e device still requires routing. IPsec policies are used only for negotiation; the encrypted traffic still relies on the route table.

IPsec Parameters

The IPsec parameters define the following:

- Default and maximum lifetimes for an IPsec security association (SA). (The defaults are 8 hours and 24 hours, respectively.)
- Diffie-Hellman group to use for session key exchange. (The default provides for automatic negotiation of the DH group.)

To change IPsec parameter values, enter the following command:

```
> config ipsec parameters
```

Table 58 describes the parameters of **`config ipsec parameters`**.

Table 58. IPsec Parameters

Parameter	Description
`lifetime`	Default IPsec SA lifetime (in seconds). The initial setting is **28800** (8 hours).
`maxlifetime`	Maximum IPsec SA lifetime (in seconds). The initial setting is **86400** (24 hours).
`group`	Diffie-Hellman group to use for session key exchange (**dh1024** | **dh768** | **nopfs** | **auto**). Use the value **nopfs** to disable *perfect forward secrecy*. The default is **auto**.

Show IPsec Parameters

To show the IPsec parameter settings, enter the following command:

```
> show ipsec parameters

IPSEC Parameters:
   Lifetime            28800 seconds
   Maximum Lifetime    86400 seconds
   DH Group            auto
```

IPsec Proposals

An IPsec proposal is a set of security parameters used when negotiating an IPsec SA with a remote secure gateway. IPsec proposals are used by the IPsec policies that reference them.

The initial BSGX4e configuration provides a predefined IPsec proposal named *VPN-A*. This predefined IPsec proposal conforms with the recommendations for a standard IPsec cryptographic suite called **VPN-A**, as described in RFC 4308.

Configuration Requirements

The BSGX4e only supports IPsec proposals that use:

- ESP protocol
- Lifetype of seconds

You must configure the IPsec proposal at the remote secure gateway to use these options.

Configuration Commands

To configure an IPsec proposal, enter the following command:

```
> config ipsec proposal
```

Table 59 describes the parameters of **config ipsec proposal**.

Table 59. IPsec Proposal Parameters

Parameter	Description
[**name**]	Name for this proposal.
encrypt	Encryption algorithm (**3DES** | **AES**). The default is **3DES**.
auth	Authentication method (**MD5** | **SHA**). The default is **SHA**.

To see an example that uses the predefined IPsec proposal **VPN-A**, see "VPN Configuration Examples" (page 163).

Show IPsec Proposals

To see the existing IPsec proposals, enter the following command:

```
> show ipsec proposal

IPSEC Proposals:
Name       Protocol   Encryption Authentication
-----------------------------------------------------------
VPN-A      ESP        3DES       SHA
```

IPsec Policies

An IPsec policy specifies the two secure networks that a VPN connects and the security parameters used to protect traffic between the two networks.

The configuration of an IPsec policy also configures an IP interface for the policy. The IP interface is assigned a name vpn*n*, such as vpn0, and requires configuration like any other IP interface.

IPsec Policy Requirements

- The IP address of the remote secure gateway in an IPsec policy must also appear as the **peer** in an IKE preshared key record.
- The VPN interface must be assigned an **IP address**.
- A **route** must send traffic to the VPN interface.
- A **firewall policy** must allow traffic on the VPN interface.
- A firewall policy must allow **ESP traffic** from the remote secure gateway. (IP packets sent from the remote secure network to the local secure network are encrypted as ESP packets.)
- A firewall policy must allow IP packets sent from the local secure network to the remote secure network. Otherwise, ESP packets cannot be routed to the remote secure gateway.

For examples of commands that carry out these policy requirements, see "VPN Configuration Examples" (page 163).

NOTE: By default, the Intrusion Detection Service (IDS) trusts a VPN interface that has been assigned an IP address and does not attempt to detect spoof attacks in its traffic. For more information, see "Spoof Protection" (page 147).

Configure IPsec Policy Command

The IPsec policy defines the IP addresses for the VPN, including the address of the remote gateway and the local and remote subnets secured by the VPN. An incoming packet whose source address matches a secure local IP address, and whose destination address matches a secure remote IP address, is encrypted and forwarded to the gateway address.

To configure an IPsec policy, enter the following command:

```
> config ipsec policy
```

Table 60 describes the parameters for **config ipsec policy**.

Table 60. IPsec Policy Parameters

Parameter	Description
[**name**]	Name for this VPN.
gateway	IP address of the remote gateway.
local	Local IP addresses secured by the VPN (**any** or addresses specified as a range or as a subnet).

Table 60. IPsec Policy Parameters (continued)

Parameter	Description
remote	Remote IP address secured by the VPN (**any** or addresses specified as a range or as a subnet).
prop	Name of the IPsec proposal. One predefined proposal is available—**VPN-A.**

Policy Configuration Example

The following command configures a policy that secures traffic for all local and remote addresses and forwards it to the gateway address 172.28.16.20:

```
> config ipsec policy Remote2 gateway 172.28.16.20 local any
remote any prop VPN-A
```

Show IPsec Policies

To show the configured IPsec policies, enter the following command:

```
> show ipsec policy

IPSEC Policy Settings:

Name              Local                              Proposal
Gateway           Remote                             Interface
-------------------------------------------------------------
Remote2           any                                VPN-A
172.28.16.20      any                                vpn1
Remote            192.168.1.0/255.255.255.0          VPN-A
194.23.7.34       192.168.2.0/255.255.255.0          vpn0
```

The `Interface` field lists the IP interface assigned to the policy (`vpn0`).

Show IPsec Security Associations

To show the current IPsec security associations (SAs), enter the following command:

```
> show ipsec sa

IPSEC SAs:
Policy      SPI         Protocol  Auth      Initiator Cookie
Initiator   Direction   Encrypt   Duration  ResponderCookie
-------------------------------------------------------------------------------
Remote      0x7200F0C   ESP       SHA       0xAE9ADE9C50F153A4
Yes         OUTBOUND    3DES      3126      0x74F586C014392273
Remote      0x9E8ACA6   ESP       SHA       0xAE9ADE9C50F153A4
Yes         INBOUND     3DES      3126      0x74F586C014392273
```

The above example shows the security associations for one IPsec policy (`Remote`). It lists security associations for both `OUTBOUND` and `INBOUND` directions.

NOTE: A tunnel can be up only if security associations are shown for both directions (`OUTBOUND` *and* `INBOUND`*).*

Clear IPsec Security Associations

To clear the current IPsec security associations (SAs), enter the following command:

```
> clear ipsec sa
```

NOTE: The clear ipsec sa command clears all IPsec SAs

IPsec Statistics

Statistics are kept to record the number of packets that IPsec receives, transmits, and drops. Counts are provided for inbound packets and for outbound packets.

To see the IPsec statistics, enter the following command:

```
> show protocol esp

ESP Stats:
Inbound Received        0          Outbound Received       0
Inbound Transmitted     0          Outbound Transmitted    0
Inbound Dropped         0          Outbound Dropped        0
Bad SPI                 0
```

The `Bad SPI` statistic counts the ESP packets received with SPI that do not match the SA.

VPN Configuration Examples

An IPsec tunnel is assigned an IP interface when its policy is configured. You can assign an IP address subnet to this interface in the same way as other IP interfaces (see "WAN Interface Configuration" (page 91) and "Firewall Security Policies" (page 130)).

To send WAN traffic through the tunnel, the traffic is routed out of the IP interface assigned to the tunnel. (The traffic is encrypted before it is sent.) The IP interface allows features such as the VoIP session controller and user agent to be used across the VPN.

Office-to-Office VPN Example

This example configuration sets up a VPN between two BSG devices. It is assumed that the two devices each control a LAN, one at the main office and the other at a branch office.

This VPN example uses the default settings for IPsec and IKE parameters and the default IPsec proposal **VPN-A**:

Shared key value: `x359QWa78b3l12`.

Main office IP addresses:

- Main office gateway: `195.178.11.11`

- Main office LAN subnet: `192.168.1.0/24`

Branch office IP addresses:

- Branch office gateway: `194.23.7.34`
- Branch office LAN subnet: `192.168.2.0/24`

Perform the following steps to configure the VPN between the two BSG devices.

1. **Log on to the BSG device at the main office.**

2. **Configure the VPN at the main office.**

3. Specify the key shared with the branch gateway by using the following command:

```
> config ike preshared 194.23.7.34 key x359QWa78b3l12
```

4. Specify the IPsec proposal (**VPN-A**) and the LAN subnets to be connected by the VPN by using the following command:

```
*> config ipsec policy Branch gateway 194.23.7.34 prop VPN-A
local 192.168.1.0/24 remote 192.168.2.0/24
```

5. **Determine the IP interface assigned to the VPN** by using the following command**:**

```
*> show ipsec policy

IPSEC Policy Settings:

Name            Local                 Proposal
Gateway         Remote                Interface
-------------------------------------------------------------
Branch            192.168.1.0             VPN-A
194.23.7.34       192.168.2.0             vpn0
```

6. **Configure the firewall at the main office to allow IPsec and IKE traffic.**

7. Define a security policy to allow traffic from the main office LAN to the VPN by using the following command:

```
*> config security policy new from eth1 to vpn0
```

8. Define a firewall security policy to allow IKE negotiation with the branch gateway (UDP traffic to port 500) by using the following command:

```
*> config security policy new from eth0 to self sip
194.23.7.34 dport 500 proto udp
```

9. Define a security policy to allow encrypted traffic from the branch gateway (ESP packets) by using the following command:

```
*> config security policy new from eth0 to self sip
194.23.7.34 proto esp
```

10. **Configure the VPN IP interface.**

11. Assign an IP subnet to the IP interface of the tunnel (**vpn0**) by using the following command. Currently, any IP subnet can be assigned to the *vpn* interface; the IP address assignment does not determine the traffic on the interface.

```
*> config interface ip vpn0 ip 10.10.10.1/24
```

12. Define a route that sends branch office traffic out of the VPN interface by using the following command:

```
*> config route table 192.168.2.0/24 if vpn0
```

13. **Save the configuration** by using the following command:

```
*> save
```

14. **Log on to the BSG device at the branch office.**

15. **Configure the branch office VPN to mirror the main office VPN.**

16. Specify the key shared with the main gateway by using the following command:

```
> config ike preshared 195.178.11.11 key x359QWa78b3l12
```

17. Specify the IPsec proposal (**VPN-A**) and the LAN subnets to be connected by the VPN by using the following command:

```
*> config ipsec policy Head gateway 195.178.11.11 prop
VPN-A local 192.168.2.0/24 remote 192.168.1.0/24
```

18. **Determine the IP interface assigned to the VPN** by using the following command:

```
*> show ipsec policy
IPSEC Policy Settings:

Name            Local                 Proposal
Gateway         Remote                Interface
-------------------------------------------------------------
Head              192.168.2.0             VPN-A
195.178.11.11     192.168.1.0             vpn0
```

19. **Configure the firewall at the branch office to allow IPsec and IKE traffic.**

20. Define a security policy to allow traffic from the main office LAN to the VPN by using the following command:

```
*> config security policy new from eth1 to vpn0
```

21. Define a firewall security policy to allow IKE negotiation with the main gateway (UDP traffic to port 500) by using the following command:

```
*> config security policy new from eth0 to self sip
195.178.11.11 dport 500 proto udp
```

22. Define a firewall security policy to allow encrypted traffic from the main gateway (ESP packets) by using the following command:

```
*> config security policy new from eth0 to self sip
195.178.11.11 proto esp
```

23.Configure the VPN IP interface.

24. Assign an IP subnet to the IP interface of the tunnel (**vpn0**) by using the following command. Currently, any IP subnet can be assigned to the *vpn* interface.

```
*> config interface ip vpn0 ip 10.10.10.2/24
```

25. Define the default route to send traffic out the VPN interface by using the following command. All traffic without another explicit route uses the default route.

```
*> config route table 0.0.0.0 if vpn0
```

26.Save the configuration by using the following command:

```
*> save
```

ISP Tunnel Example

This example shows an IPsec tunnel configured from the BSGX4e WAN interface to the VPN gateway of the ISP.

The VPN uses the settings of the default IPsec proposal **VPN-A**. The shared key value is `x232skd24scefk3o`. The IP addresses used are:

- **BSGX4e**: `192.168.100.1`
- **ISP**: `192.168.100.2`
- **VPN gateway at ISP**: `10.254.254.254`

To configure the tunnel, perform the following steps.

1. Configure the VPN in the BSGX4e.

2. Specify the preshared key for the remote gateway by using the following command:

```
> config ike preshared 10.254.254.254 key x232skd24scefk3o
```

3. Specify the IPsec proposal (**VPN-A**) and the IP addresses of the traffic routed through the tunnel by using the following command:

```
*> config ipsec policy Tunnel gateway 10.254.254.254 prop
VPN-A local 192.168.100.1 remote 192.168.100.2
```

4. Determine the IP interface assigned to the tunnel by using the following command:

```
*> show ipsec policy

IPSEC Policy Settings:

Name            Local                   Proposal
Gateway         Remote                  Interface
-----------------------------------------------------------------
Tunnel            192.168.100.1             VPN-A
10.254.254.254    192.168.100.2             vpn0
```

5. Assign an IP address to the IP interface of the tunnel (vpn0) by using the following command:

```
*> config interface ip vpn0 ip 192.168.100.1
```

6. **Enable NAT on the tunnel interface** by using the following command:

```
*> config security nat interface vpn0 status on
```

7. **Define a default route for the tunnel interface** by using the following command**.** This route sends all traffic on the tunnel unless the traffic has another explicit route. This also applies to VoIP traffic.

```
*> config route table 0.0.0.0 if vpn0
```

8. **Configure the firewall to allow tunnel traffic.**

9. Allow traffic from the LAN to the tunnel by using the following command:

```
*> config security policy new from eth1 to vpn0
```

10. Allow IKE negotiation (UDP traffic to port 500 from the remote gateway) by using the following command:

```
*> config security policy new from eth0 to self sip
10.254.254.254 dport 500 proto udp
```

11. Allow IPsec traffic (ESP traffic from the remote gateway) by using the following command:

```
*> config security policy new from eth0 to self sip
10.254.254.254 proto esp
```

12. Allow ICMP packets to come in from the tunnel by using the following command:

```
*> config security policy new from vpn0 to self proto icmp
```

13. **Save the configuration** by using the following command:

```
*> save
```

Configuring the ISP Gateway

For the tunnel to the ISP to be usable, you must configure the ISP gateway in a compatible manner to accept the traffic from the BSGX4e and to forward it on.

If the ISP gateway (the remote gateway) is an BSG unit, you can use the following commands as a starting point for its VPN configuration. The following example assumes that the gateway address is **10.0.0.1**.

1. **Configure the VPN.**

2. Specify the same preshared key used by the gateway at the other end of the tunnel.

```
> config ike preshared 10.0.0.1 key x232skd234scefk3o
```

3. Configure the IPsec policy for the tunnel. Specify an IPsec proposal compatible with **VPN-A** (ESP protocol, 3DES encryption, and SHA authentication).

```
*> config ipsec policy Tunnel gateway 10.0.0.1 prop VPN-A
local 192.168.100.2 remote 192.168.100.1
```

4. **Determine the IP interface assigned to the tunnel by using the following command:**

```
*> show ipsec policy

IPSEC Policy Settings:

Name              Local                    Proposal
Gateway           Remote                   Interface
-------------------------------------------------------------
Tunnel             192.168.100.2              VPN-A
10.0.0.1           192.168.100.1              vpn0
```

5. **Assign an IP address to the IP interface of the tunnel (vpn0) by using the following command:**

   ```
   *> config interface ip vpn0 ip 192.168.100.2
   ```

6. **Define a default route for the tunnel interface.** This route sends all traffic on the tunnel unless the traffic has another explicit route.

   ```
   *> config route table 0.0.0.0 if vpn0
   ```

7. **Configure the firewall to allow tunnel traffic.**

8. Allow traffic from the LAN to the tunnel by using the following command:

   ```
   *> config security policy new from eth1 to vpn0
   ```

9. Allow IKE negotiation (UDP traffic to port 500 from the remote gateway).

   ```
   *> config security policy new from eth0 to self sip
   10.0.0.1 dport 500 proto udp
   ```

10. Allow IPsec traffic (ESP traffic from the remote gateway).

    ```
    *> config security policy new from eth0 to self sip
    10.0.0.1 proto esp
    ```

11. **Save the configuration by using the following command:**

    ```
    *> save
    ```

Configuring a VPN

This section describes the steps for setting up VPNs to secure traffic between branch and head offices.

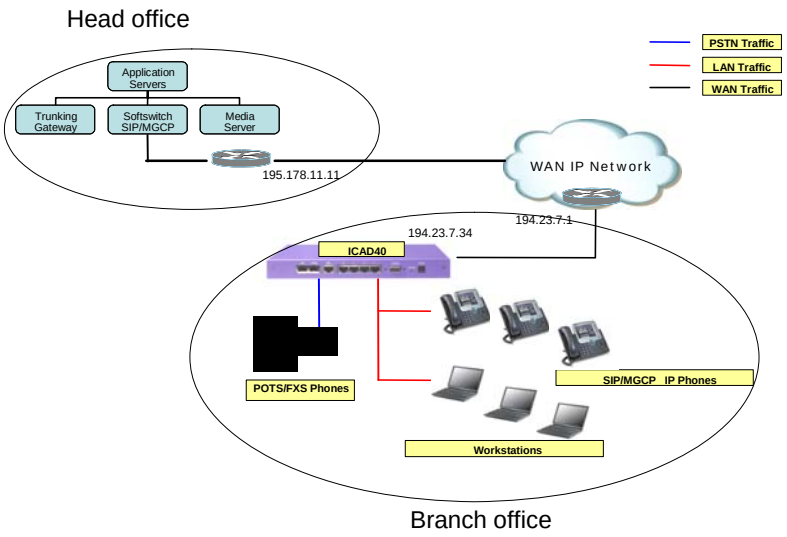


Figure 3 Head office and branch office traffic

Table 61 describes network information

Table 61. Network information

BRANCH OFFICE	**LAN IP Range**	192.168.2.0/24 192.168.2.1 (BSGX4e)
	WAN IP Range	194.23.7.0/16 194.23.7.34 (BSGX4e)
HEAD OFFICE	**LAN IP Range**	192.168.1.0/24 192.168.1.1 (Cisco 3845)
	WAN IP Range	195.178.11.0/24 195.178.11.11 (Cisco 3845)

Configuration guidelines describe an actual case for configuring an BSGX4e for deployment at a small customer office to implement a complete secure Voice over Internet Protocol (VoIP) (Session Initiated Protocol (SIP) environment) and data solution:

- The SIP Session Controller (SIP SC) controls VoIP telephones are installed in the LAN network. The SIP User Agent (SIP UA) controls an analog fax machine is attached to the FXS port of the BSGX4e.
- Workstations installed in the LAN access various data services such as e-mail, chat, and the World Wide Web.
- Head office exchanges all VoIP and data traffic traffic. Traffic is plain routed and encrypted.

To configure the VPN on the BSGX4e, you must understand how VoIP and data flows go through the BSGX4e. Figure 4 shows the logical path of flows of the routing engine.

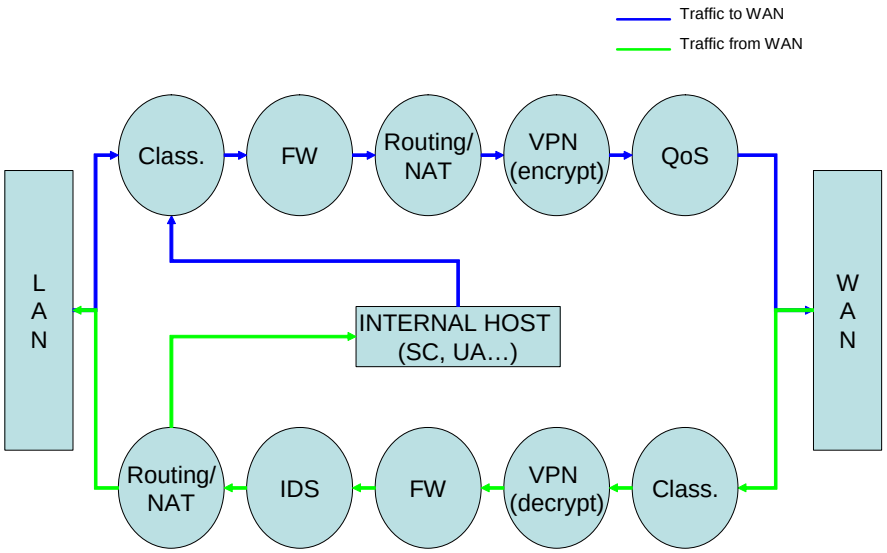


Figure 4 Logical path of the routing engine

Flows are exchanged between three components: equipment located in LAN, equipment located in Wide Area Network (WAN), and the internal host handling services such as the Session Controller and the User Agent.

Traffic to the WAN goes through the Classifier, Firewall (FW), Routing/NAT, VPN (to encrypt packets) and Quality of Service (QoS). Traffic from the WAN goes through the Classifier, VPN (to decrypt packets), Firewall, Intrusion Detection System (IDS), and Routing/NAT. Assume that traffic to the WAN is trusted, so it does not need to be checked by the Intrusion Detection System. Traffic from the WAN usually has a low speed, so there is not a strong need for QoS. The traffic classification happens once as soon as the traffic comes in the routing engine. As a consequence, it runs while packets are not yet modified by routing, NAT, or VPN. The results of the classification apply to all subsequent modules in the path (such as Firewall, VPN, or QoS). This means QoS classification applies on clear packets, but not on encrypted

packets, even if QoS operates after VPN. If packets that must be sent to the WAN are bigger than the Maximum Transmission Unit (MTU) of the WAN interface after encryption, the routing stacks fragments before encryption.

As described in diagram 1, the packets sent to the WAN are encrypted before QoS treatments are applied. The QoS stack needs to know how packets are modified by the encryption (packets are bigger) in order to calculate what exactly will be sent to the wire. The performance that can be expected depends on the different modules.

Table 62 reports them in packets per second (pps). Performances tests (RFC 2544) have all been done in bidirectional mode.

Table 62. Performance of each module with QoS running concurrently

Packet size (bytes)	64	128	256	512	1024	1280	1518
Classifier							
LAN-WAN	148810	84460	45290	23497	11973	9616	8128
WAN-LAN	148810	84460	45290	23497	11973	9616	8128
FW							
LAN-WAN	148810	84460	45290	23497	11973	9616	8128
WAN-LAN	148810	84460	45290	23497	11973	9616	8128
Routing/NAT							
LAN-WAN	148810	84460	45290	23497	11973	9616	8128
WAN-LAN	148810	84460	45290	23497	11973	9616	8128
IDS							
LAN-WAN	127000	84460	45290	23497	11973	9616	8128
WAN-LAN	90000	84460	45290	23497	11973	9616	8128
VPN							
LAN-WAN	45620	39308	28506	19260	10984	9104	4500
WAN-LAN	45620	39308	28506	19260	10984	9104	4500
QoS							
LAN-WAN	106838	84460	45290	23497	11973	9616	8128
WAN-LAN	106838	84460	45290	23497	11973	9616	8128

The slowest module is VPN. Performance is good for small packets because they are processed only in the hardware assist engine. Large packets result in low performance because the Central Processing Unit (CPU) does fragmentation before starting encryption. Sending more than what is supported leads to unexpected packet loss.

Encryption and decryption work based on the routing table. They do not work based on the IPSec policies. They are only used to negotiate Internet Key Exchange (IKE) phase 2. A slight difference exists depending on whether you use NAT. If you do not use NAT, the processes work as follows:

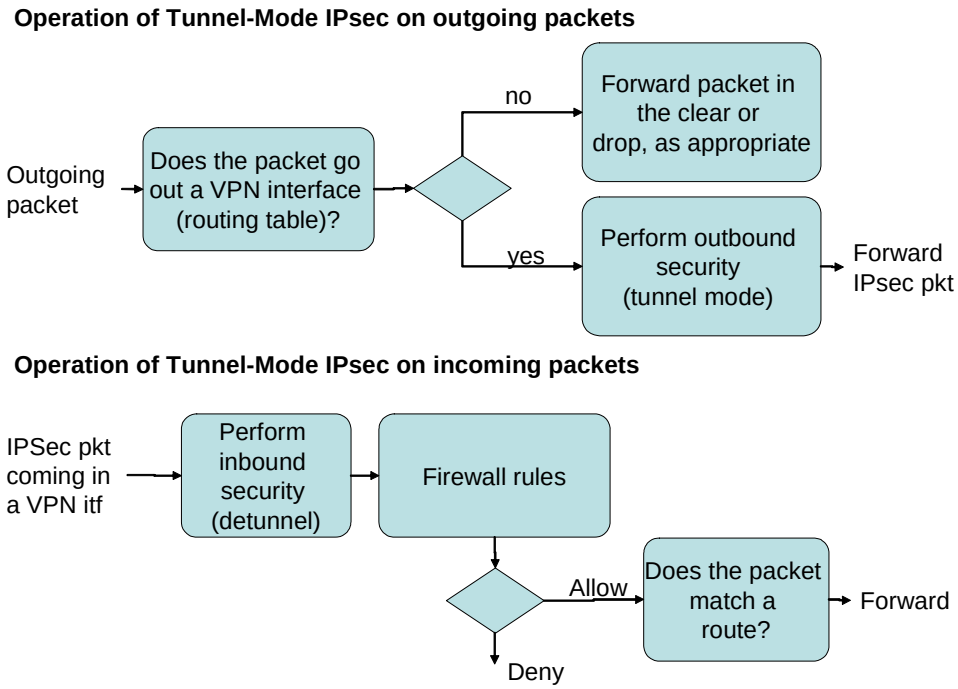

Operation of Tunnel-Mode IPsec on outgoing packets
Outgoing packet
Does the packet go out a VPN interface (routing table)?
no
Forward packet in the clear or drop, as appropriate
yes
Perform outbound security (tunnel mode)
Forward IPsec pkt
Operation of Tunnel-Mode IPsec on incoming packets
IPSec pkt coming in a VPN itf
Perform inbound security (detunnel)
Firewall rules
Allow
Does the packet match a route?
Forward
Deny

Figure 5 VPN operations when NAT is disabled

If NAT is enabled, the processes work as below:

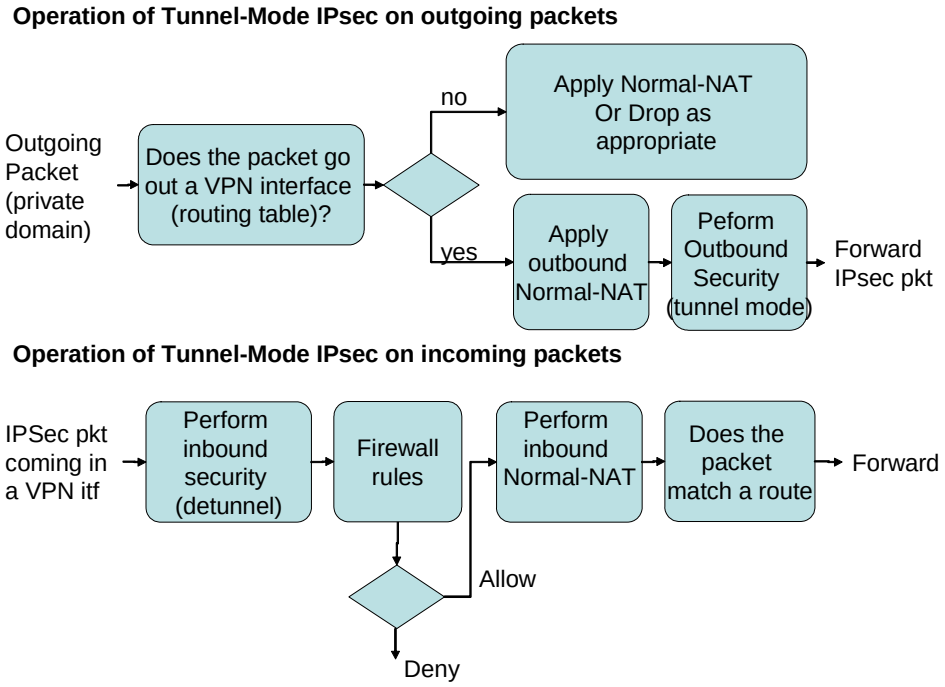

Operation of Tunnel-Mode IPsec on outgoing packets
Outgoing Packet (private domain)
Does the packet go out a VPN interface (routing table)?
no
Apply Normal-NAT Or Drop as appropriate
yes
Apply outbound Normal-NAT
Peform Outbound Security (tunnel mode)
Forward IPsec pkt
Operation of Tunnel-Mode IPsec on incoming packets
IPSec pkt coming in a VPN itf
Perform inbound security (detunnel)
Firewall rules
Perform inbound Normal-NAT
Does the packet match a route
Forward
Allow
Deny

Figure 6 VPN operations when NAT is enabled

You must understand how traffic is flowing through the unit to understand how traffic is encrypted. Figure 7 shows this flow.

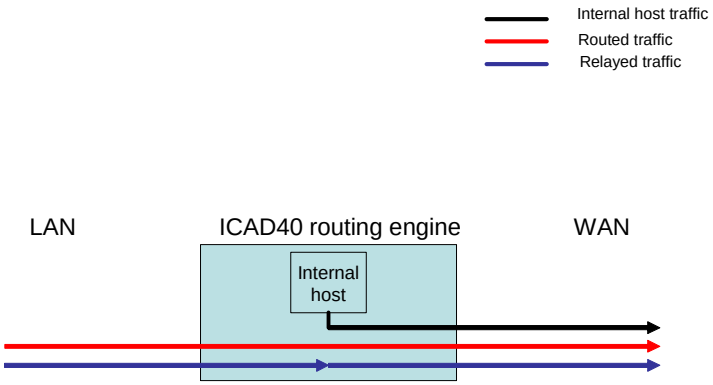


Figure 7 Flow types

Three flow types can be distinguished:

- Internal host traffic: this is the traffic terminating at the unit. The source IP address of the packets sent that for encryption is that of the egress VPN interface of the unit. It concerns the services run by the internal host such as Telnet, RADIUS Web, and Simple Network Management Protocol (SNMP).
- Routed traffic: this is the traffic normally routed by the unit. If you do not use NAT, the source IP addresses of the packets sent for encryption are the original ones. If you use NAT, the source (public) IP address is that of the egress VPN interface of the unit. It concerns traffic using File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), or Hypertext Transfer Protocol (HTTP).
- Relayed traffic: this traffic terminates at the unit before being sent for encryption. This means the destination IP address of the packets sent from LAN is the LAN IP address of the unit. These packets are relayed to the WAN. The source IP address of the packets is that of the egress VPN interface of the unit. It concerns 4 types of traffic: VoIP, TFTP (using relay), Domain Name Service (DNS) (using relay) and SNTP (using relay). For VoIP traffic, the Session Controller modifies the Session Description Protocol (SDP) bodies of the signalling messages in order to make the VoIP endpoints send their traffic to the unit in order to relay them. For TFTP, DNS, and SNTP, data endpoints located on the LAN are configured with the LAN IP address of the unit. Requests received are then relayed to the WAN to the right servers (found in the configurations of the relay functions).

VPN support on BSGX4e

The BSGX4e Business Gateway supports IPSec for securing IP communications by encrypting and authenticating all packets at the network layer. Up to 10 tunnels can be setup concurrently. Tunnel mode is supported. Encryption can be 3DES (168) or AES (128, 192, and 256). Authentication can be SHA (96) or MD5 (96).

Use IKE to set up IPSec Security Associations (SA). IKE uses a preshared key. Encryption can be DES (56), 3DES (168), AES (128, 192, and 256) or BLOWFISH (128). Authentication can be SHA or MD5.

There are two types of SA.

1. IKE SAs: Established during IKE main mode negotiations, IKE SAs determine how to secure subsequent IKE negotiations between the secure gateways.
2. IPSec SAs: Established during IKE quick mode negotiations, IPSec SAs determine how to secure IP traffic between the offices (LANs).

SAs are dynamic in nature. They are automatically negotiated when the first attempt to send an IP packet between offices (LANs) is made. SAs expire after a finite time, although prior to expiry a replacement SA is automatically negotiated.

Once IPSec SAs are established, the VPN becomes operational, and secure gateways use IPSec tunneling to secure IP traffic between offices (LANs). IP packets are sent between offices (LANs) securely encrypted inside an Encapsulated Security Payload (ESP) packet during transmission between the secure gateways.

Setting up a VPN requires that you configure both IKE and IPSec.

Packets are encrypted and decrypted by a hardware assist engine allowing both VoIP and data traffic to be securely conveyed through IP networks.

Example

This example shows how to deploy VPN to secure VoIP and data traffic with a Cisco router 3845. Plain routed is implemented.

Analyze

The difficulty to interoperate with a Cisco router when running a plain routing through an IPSec tunnel is that the BSGX4e does not use the same source IP addresses depending on the traffic forwarded. Traffic normally routed, such as FTP, TFTP, and HTTP, is forwarded with the LAN source IP addresses unchanged. Relayed traffic such as SIP, TFTP, SNTP, and DNS is forwarded with the IP address assigned to the VPN interface as the source IP address.

IPSec does not work exactly the same on the BSGX4e and a Cisco router:

- The IPSec policies (ipsec policy) configured on the BSGX4e are not used at all for encryption/decryption. No checking is done. Encryption is based on the routing table only (in other words, if it must be sent over a VPN interface). Decryption is based on which interface the ESP packets are received (in other words, if it received on a VPN interface).
- The IPSec policies (access-list or crypto map) configured on a Cisco router are used to check encryption/decryption. Encryption is based on these policies (you cannot encrypt traffic that does not match these policies). Decryption is based on these policies (decrypted traffic not matching these policies is discarded).

There is only one IPSec policy per tunnel, so this one policy must match both traffic types (traffic plain routed and relayed traffic) exchanged between the BSGX4e and the Cisco router. Another solution is to setup two tunnels, one for the traffic plain routed, one for the relayed traffic (note that it would be the same for NATed traffic).

Configuration of BSGX4e using a single tunnel

1. Configuring the IKE.

Configure the IKE preshared key (CA certificates are not supported).

```
BSG> config ike preshared 195.178.11.11 Key MyKey
```

UDP 500 does IKE negotiation. Configure the firewall to allow IKE.

```
BSG> config security policy new From eth0 To self DPort 500
Proto udp sip 195.178.11.1
```

Optionally, you can configure the IKE lifetime. When the lifetime timer expires, the IKE SA is renegotiated as a security measure.

```
*BSG*> config ike parameters LifeTime 86400 MaxLifeTime
       259200
```

2. Configuring IPSec.
Configure IPSec encryption and authentications algorithms, 3DES/SHA as follows. This creates the vpn interface vpn0.

```
*BSG*> conf ipsec proposal 3DES-SHA encrypt 3DES auth SHA
*BSG*> config ipsec policy cisco Gateway 195.178.11.11
Local 0.0.0.0/0.0.0.0 Remote 192.168.1.0/24 Prop 3DES-SHA
```

NOTE: By setting local to any, it forces the Cisco router to accept any packets (plain routed or relayed) coming from the BSGX4e to be decrypted. Also it forces the Cisco router to encrypt any packets intended for the BSGX4e (configured in the routing table).

Configure the firewall to allow IKE.

```
*BSG*> config security policy new From eth0 To self Proto
esp sip 195.178.11.11
```

Optionally, you can configure the IPSec session lifetime. When the lifetime expires, the session renegotiates the IPSec SA as a security measure.

```
*BSG*> config ipsec parameters LifeTime 28800 MaxLifeTime
86400
```

Optionally, you can configure the DH group to use for session key exchange.

```
*BSG*> config ipsec parameters group auto
```

3. Configuring routing.
Configure the IP address (20.0.0.1 for example) of the interface vpn0 in order to relay traffic.

```
*BSG*> config interface ip vpn0 ip 20.0.0.1/255.255.255.0
```

To reach the remote LAN, go through the VPN interface.

```
*BSG*> config route table 192.168.1.0/255.255.255.0 if vpn0
```

Configure the firewall to allow traffic coming from the LAN to be sent through the tunnel.

```
*BSG*> config security policy new From eth1 To vpn0
```

Configuration of Cisco

1. Configuring IKE.
Configure the IKE preshared key.

```
cisco> crypto isakmp policy 1
   encr 3des
   authentication pre-share
   group 2
cisco> crypto isakmp key MyKey address 194.23.7.34
```

2. Configuring IPSec.
Configure the tunnel for 3DES-SHA.

```
cisco> crypto ipsec transform-set BSGX4e-Cisco3845-IPSEC
esp-3des esp-sha-hmac
```

Configure a symmetrical IPSec policy.

```
cisco> access-list 101 permit ip 192.168.1.0 0.0.0.255 any
cisco> crypto map BSGX4e-Cisco3845 1 ipsec-isakmp
    set peer 194.23.7.34
    set transform-set BSGX4e-Cisco3845-IPSEC
    match address 101
```

NOTE: By setting this, you force the Cisco router to accept any packets (plain routed or relayed) coming from the BSGX4e to be decrypted.

3. Configuring routing.
Assign the IKE/IPSec configuration to the WAN interface of the Cisco router (ge 0/0 in this case).

```
cisco> interface GigabitEthernet0/0
    crypto map BSGX4e-Cisco3845
```

Configure a route for plain routed traffic.

```
*BSG*> ip route 192.168.2.0 255.255.255.0 194.23.7.34
```

Configure a route for relayed traffic.

```
*BSG*> ip route 20.0.0.1 255.255.255.255 194.23.7.34
```

NOTE: By setting this, you force the Cisco router to encrypt any packets intended for the BSGX4e.

Troubleshooting on BSGX4e

1. Is IKE SA successfully negotiated?
The command show ike sa reports the status of this negotiation. If the negotiation fails, no entry is displayed.

```
BSG> show ike sa
IKE SAs:

LocalAddr        Group     Encryption Duration InitiatorCookie
RemoteAddr       Initiator Hash       LifeType ResponderCookie
-------------------------------------------------------------------------
194.23.7.34      DH1024    3DES       78752    0x8094844CC8D21555
195.178.11.11    Yes       SHA        Seconds  0x57259F0354BDE231
```

The number of IKE packets exchanged can be displayed.

```
BSG> show protocol ike
IKE Stats:
Packets Sent      8                      Packets Received     6
Events Sent      13                      Events Received      13
```

2. Is IPSec SA successfully negotiated?

The command show ipsec sa reports the status of this negotiation. An entry for each direction (INBOUND and OUTBOUND) of the tunnel must be displayed. If the negotiation fails, no entry is displayed.

```
BSG> show ipsec sa
IPSEC SAs:

Policy    SPI        Protocol Auth     InitiatorCookie
Initiator Direction  Encrypt  Duration ResponderCookie
------------------------------------------------------------
cisco     0x59078E14 ESP      SHA      0x8094844CC8D21555
Yes       OUTBOUND   3DES     6470     0x57259F0354BDE231
Cisco     0x9DCED3E4 ESP      SHA      0x8094844CC8D21555
Yes       INBOUND    3DES     6470     0x57259F0354BDE231
```

3. Are packets going through the tunnel?

The command show protocol esp reports the number of packets encrypted and the number of packets decrypted. After traffic goes through this tunnel and it is administratively up. This ensures the tunnel is working.

```
BSG> show protocol esp
ESP Stats:

Inbound Received        1556            Outbound Received        1557
Inbound Transmitted     1556            Outbound Transmitted     1557
Inbound Dropped            0            Outbound Dropped         0
Bad SPI                    0
```

Table 63. ESP Statistics

Counter	Definition
Inbound Received	number of packets received by the crypto engine to be decrypted
Inbound Transmitted	number of packets sent to the routing stack by the crypto engine after decryption
Outbound Received	number of packets received by the crypto engine to be encrypted
Outbound Transmitted	number of packets sent to the crypto engine by the routing stack for encryption
Inbound Dropped	number of packets dropped during decryption
Bad SPI	number of packets dropped during decryption because of an unknown SPI
Outbound Dropped	number of packets dropped during encryption

11 GoS Configuration

This chapter describes how to configure the advanced Quality of Service (QoS) feature in the BSGX4e. This feature is called Guarantee of Service™ or GoS™.

GoS is based on network layer 3. The BSGX4e also supports layer 2 QoS, which allows the user to prioritize LAN traffic as it enters the device. For information on layer 2 QoS, see "Layer 2 QoS" (page 106).

Introduction to GoS

The BSGX4e device uses Nortel's patented QoS technology, GoS™, to deliver reliable quality of service. GoS is designed for the convergence of voice calls and other real-time services with data traffic. It allows for prioritization of traffic from multiple applications based on the particular loss and delay sensitivities of each application.

GoS can do the following:

- **Manage Contention**

  In typical installations, the BSGX4e device is deployed at the customer premises, at the boundary between the high bandwidth LAN and the lower bandwidth WAN. Network contention occurs at this point, where Fast Ethernet traffic from the LAN competes for access to the WAN connection.

Figure 8. Capacity Reduction Between Fast Ethernet and WAN

- **Protect Voice Traffic**

  Voice streams, in particular, are sensitive to quality degradation. Real-time calls cannot tolerate high packet delay (and, to a lesser extent, high packet loss). Therefore, voice traffic must be given higher priority to the WAN connection.

  GoS is integrated with the VoIP session controller so that bandwidth is allocated for voice traffic as calls are established. For more information about the session controller, see "SIP Configuration" (page 263) or "MGCP Configuration" (page 209).

GoS can provide:

- Guaranteed bandwidths with enforced bandwidth limits and reuse of unclaimed bandwidth. This feature provides network stability under an increasing load.
- Separate control of loss and delay priorities.
- Fair sharing of quality, not just bandwidth.

  No stream is allowed to use excessive network resources. This enhances the IDS protection against denial of service attacks and similar packet floods (see "Flood Protection" (page 143)).
- Live monitoring of delivered quality.

Quality Groups

A GoS quality group defines treatment parameters for the traffic streams assigned to the quality group. These treatment parameters include assignment to a GoS class that defines packet delay and packet loss priorities. The quality group also defines the bandwidth allocated and the policing method used to enforce bandwidth limits.

When more than one traffic stream has the same quality requirements you can assign the streams to the same quality group. Or, each user can be assigned to their own quality group, thus allowing for individual protection and monitoring. You can assign up to sixteen quality groups to the same GoS class.

GoS Classes

On a normal network link, before GoS control is applied, all traffic streams compete for bandwidth on a best-effort basis. With GoS control, traffic that is entitled to priority treatment automatically displaces best-effort traffic when necessary, up to its bandwidth limit. This allows spare capacity to be used freely for best-effort traffic, without affecting priority traffic.

When the link is heavily loaded, even with bandwidth control, packets are still subject to delay (because they have to queue for transmission) or, occasionally, loss (because the queue may be full). With GoS, traffic is assigned a GoS class, which defines the relative treatment that its packets receive in this case. If traffic is defined as highly sensitive to delay, its packets queue-jump less urgent traffic; if defined as highly sensitive to loss, extra queue spaces are made available.

Each class is designated by a letter, **A-C**, and a number, **1-3**. Figure 9 illustrates the relationship of GoS classes.

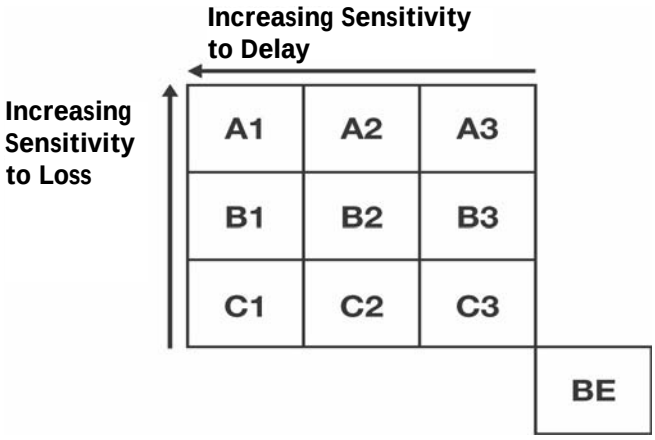


Figure 9. GoS Classes

A—C represents the range of packet loss; typically, packet loss is more acceptable for voice traffic than for data traffic.

1—3 represents the range of packet delay; typically, packet delay is more acceptable for data traffic than for voice and other real-time traffic.

Class **A1** provides the minimum loss and minimum delay of packets. Assign this class to only the most critical traffic.

BE represents best effort, a default setting that provides the lowest priority of all traffic. Within the BE group, all packet streams are given equal weight, with full access to the bandwidth that the prioritized groups are not using. A BE group has the lowest priority.

Traffic Policing

Traffic policing refers to the methods used to allocate bandwidth as the traffic rate increases. A quality group can be either policed for a strict rate or policed for a committed access rate (CAR). Strict policing enforces a strict bandwidth limit. CAR policing allows for an additional burst parameter (randomized gaps between packets), permitting available bandwidth to be taken to an upper limit.

Strict Policing

Strict policing allows the network administrator to set an absolute limit for traffic (its committed rate). Traffic that arrives at a rate below this level is allowed through and receives the loss and delay priority treatment assigned to its GoS class. Traffic that arrives above the configured rate is discarded; see Figure 10. This bandwidth is guaranteed to be available to the quality group whenever it is demanded.

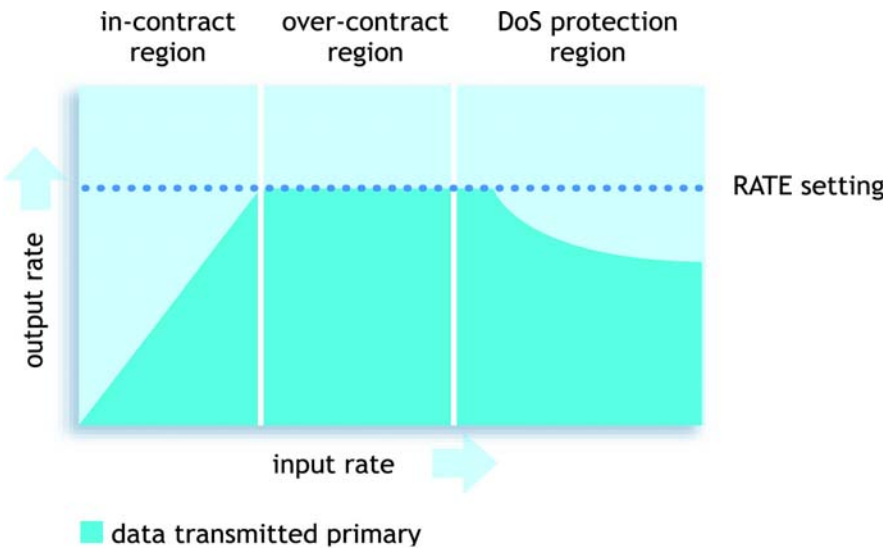


Figure 10. Strict Policing

Figure 10 also shows three regions as the input rate increases:

- the in-contract region, where the input rate is below the committed rate setting
- the over-contract region, where the input rate exceeds the committed rate setting, and so, the output rate is less than the input rate
- the denial of service (DoS) protection region, where the input rate is so great that it could be a DoS flood attack

CAR Policing

Committed Access Rate (CAR) policing provides a way for traffic in this quality group to reuse bandwidth that is assigned to other quality groups, but which is currently unused. The extra bandwidth is made available on a best-effort basis: it is not regulated and is treated with the lowest loss and delay priority.

Two parameters are set for a CAR-policed group:

- The rate setting assigns a bandwidth guaranteed exclusively to this quality group. Traffic that arrives inside this limit is prioritized according to its assigned GoS class.
- The burst setting is the maximum total bandwidth that this quality group is allowed to use when borrowing unused capacity from other groups. This extra traffic is downgraded to the best-effort GoS class.

Data that arrives in a CAR-policed quality group at a rate greater than the burst setting is discarded.

The two limits used by CAR policing (the committed rate and the burst rate) are illustrated in Figure 11.

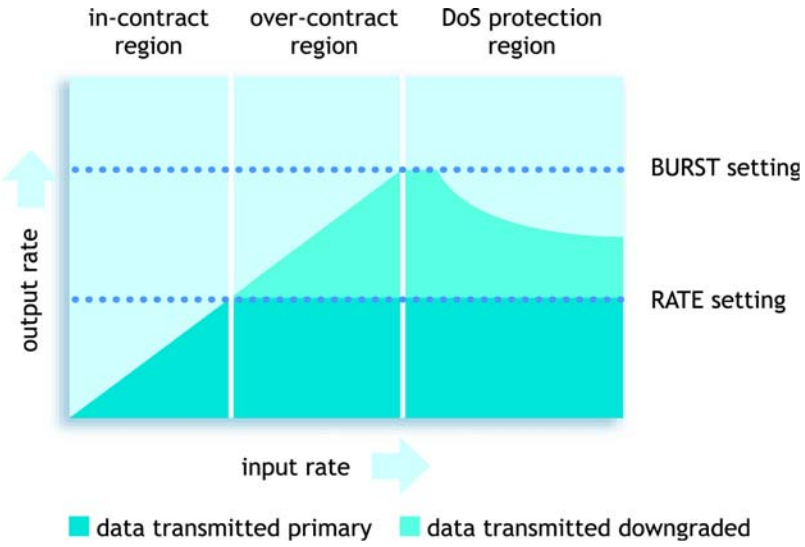


Figure 11. CAR Policing

Figure 11 also shows three regions as the input rate increases:

- the in-contract region, where the input rate is below the committed rate setting
- the over-contract region, where the input rate exceeds the committed rate setting, but is within the burst rate, and so, the data is downgraded, but forwarded if bandwidth is available
- the denial of service (DoS) protection region, where the input rate is so great that it could be a DoS flood attack

Best Effort Policing

Best Effort (BE) traffic can use whatever bandwidth is left over after non-BE traffic has been dealt with. The group can burst up to the whole capacity of the network link but is treated as lowest priority.

Configuring GoS

The configuration of GoS requires three steps:

1. **Configure a GoS link.**

   A GoS link defines the bandwidth that GoS manages for the specified interface. For example, to manage the entire bandwidth for a T1 WAN link, a GoS link is configured for the maximum rate of 1.5 Mbps.

2. **Configure GoS quality groups.**

   A quality group defines a set of quality treatment parameters, including a GoS class and a bandwidth allocation and policing method.

3. **Configure security policies to classify packets.**

A security policy defines an outgoing traffic stream and assigns it to a quality group.

Configuring a GoS Link

This section describes how to configure a GoS link. A GoS link specifies the outgoing interface whose traffic is to be managed and the size of the bandwidth to be managed—the maximum speed of that link.

NOTE: The current software release supports only one GoS link for the device.

NOTE: The GoS link is configured on the physical WAN interface, eth0. You cannot configure the GoS link on a virtual interface (vif or vpn).

To configure the GoS link, enter the following command:

```
> config qos link
```

Table 64 describes the parameters for **config qos link**.

Table 64. GoS Link Configuration Parameters

Parameters	Description
[if]	Interface to which this link applies (**eth0**).
max	Maximum speed of the link in bits per second (bps). (For an Ethernet interface, calculate this rate to include the Ethernet header but not the FCS. For example, calculate a stream of 64-byte IP packets as 78-byte packets because their Ethernet headers are included.)
comment	Optional comment describing this link.

GoS Link Example

This example configures the GoS link as follows:

Interface (WAN): `eth0`
Maximum speed (WAN bandwidth): `1.5 Mbps`
Comment (description of link): `"Office link"`

```
> config qos link eth0 max 1500000 comment "Office link"
*> save
```

Show the GoS Link

To show the GoS link configuration, enter the following command:

```
> show qos link
 QoS Links:
```

```
Interface Max             Comment
-------------------------------------------------------------
eth0      1500000         Office link
```

Delete GoS Link

NOTE: Before you can delete a GoS link, you must delete all quality groups that apply to the link. To list the quality groups, enter the command **show quality group**.

For example, the following command deletes the GoS link for the WAN interface eth0:

```
> del qos link eth0
*> save
```

Configuring Quality Groups

This section describes how to configure quality groups. A quality group is the definition of a GoS treatment, including bandwidth, policing, and GoS class.

Configuration Constraints

- The GoS link must be configured before the quality groups that reference that link.
- Ten percent of link capacity is always reserved for Best Effort traffic. Thus, no more than 90% of the maximum link rate can be explicitly committed to other quality groups. The sum of the committed rates for all other quality groups must not be greater than 90% of the link rate.

Downgraded and Dropped Packets

Consider the following when configuring GoS quality groups:

- When a quality group specifies committed access rate (CAR) policing, traffic can be downgraded and discarded, as follows:
  - Traffic received between the committed rate and the burst rate is downgraded; it becomes best effort (BE) traffic.
  - Traffic assigned to BE is forwarded only if bandwidth is available. If bandwidth is not available, the traffic is discarded; thus, the forwarding of downgraded traffic is not guaranteed.
- Traffic is always discarded if the offered load is out of contract: traffic is not forwarded if it exceeds what is guaranteed. Traffic received over the *committed* rate for a *policed* quality group or over the *burst* rate for a *CAR* quality group is always discarded.

- Traffic can be discarded even when the average theoretical throughput of the flow is within contract. This can happen when the traffic source is bursting and packets are being deterministically dropped.
- Packet loss is typically due to peak traffic; however, it can also occur if an incorrect load estimate is made.

  For example, suppose that up to fifteen VoIP calls can be set up simultaneously, but the quality group to protect VoIP traffic is sized to protect only ten calls. Calls would then be dropped because of configuration error, not because of extraordinarily high traffic. So, to avoid dropped calls, sufficient bandwidth must be protected by the quality group to accommodate the total number of possible calls.

Default Best Effort Quality Group

When a GoS link is created, a default quality group assigned to BE (best effort) is automatically created. This default quality group does not prioritize traffic, and it is not shown when you enter **show quality group**. However, this BE quality group exists to serve as default traffic manager for the traffic flows that are not assigned to any other quality group.

You can explicitly define a quality group as best effort (BE). The defined BE quality group replaces the hidden default BE group. Unlike the default BE group, a defined BE quality group does appear in the quality group list.

Quality Group Command

To configure a GoS quality group, enter the following command:

```
> config qos group
```

Table 65 describes the parameters for **config qos group**.

Table 65. GoS Group Configuration Parameters

Parameter	Description
[name]	Name of the quality group to be created or edited.
link	Interface of the link. Use this parameter if more than one GoS link is defined. The default is **eth0**.
qg	GoS class (**A1** | **A2** | **A3** | **B1** | **B2** | **B3** | **C1** | **C2** | **C3** | **BE**). The default is **BE**. You can assign up to 16 quality groups to the same GoS class. Refer to "GoS Classes" (page 182).
type	Policing method (**car** | **policed** | **besteffort**). The default is **besteffort**. Refer to "Traffic Policing" (page 183).
committed	Committed rate for the quality group (in bps). Specify a value if **qg** is *not* **BE**. The minimum rate is 64000. The maximum rate is 90% of the total link rate (as specified on **config qos link**).

Table 65. GoS Group Configuration Parameters (continued)

Parameter	Description
burst	Burst rate for the quality group (in bps). Specify a value if **type** is **car** and **qg** is *not* **BE**. Ensure that the burst rate is greater than the committed rate and less than or equal to the maximum link rate (as specified by the **config qos link**).
iptoS	IP ToS value to be written into each packet assigned to this quality group (decimal, **0-255**). Specify **no** if no ToS value is to be written. If supported by the upstream router, the ToS value can notify the router to minimize delay/cost or maximize throughput/routing. (The ToS value in downgraded packets is reset to 0 because those packets are out of contract.)
cos	CoS value to be written into each packet assigned to this quality group (decimal, **0-7**). Specify **no** if no CoS value is to be written. If supported by the upstream router, the CoS value can notify the router if VLAN traffic is to be prioritized (as defined by the IEEE 802.1p standard).

Quality Group Examples

The following examples illustrate the configuration of two quality groups. The examples assume that a GoS link is defined for the WAN interface (eth0) with a maximum rate of 1.5 Mbps. Up to 90% of that bandwidth (1.35 Mbps) can be committed to quality groups; the other 10% (150 kilobits per second (kbps)) must be left for best effort traffic.

The following two examples divide the 1.35 Mbps between two quality groups: 500 kbps is assigned to high-priority VoIP traffic; the other 850 kbps is assigned to lower-priority data traffic; however, the data traffic can burst up to the entire 1.5 Mbps bandwidth if it is available.

Example 1

This example configures a quality group for handling high-priority VoIP traffic:

Name of group: `VoIP`
Quality group class: `A1 (minimum delay, minimum loss)`
Policing method: `policed`
Committed rate: `500 000 (500 kbps)`

```
> config qos group VoIP qg A1 type policed committed 500000
*> save
```

Example 2

This example configures a quality group for handling lower-priority data traffic:

Name of group: `Data`

Quality group class: A3 (maximum delay, minimum loss)
Type of policer: CAR
Committed rate: 850 000 (850 kbps)
Burst rate: 1 500 000 (1.5 Mbps)

```
> config qos group Data qg A3 type CAR committed 850000 burst
1500000
*> save
```

Show Quality Groups

To see the currently defined quality groups, enter the following command:

```
> show qos group
```

```
QoS Quality Groups:
Name    Link      QG    Type       Committed  Burst   IPToS  COS
-------------------------------------------------------------------
VoIP    eth0      A1    policed    500000     0       no     no
Data    eth0      A3    car        850000     1500000 no     no
```

Delete a Quality Group

To delete a quality group, specify the group name on a **del qos group** command.

NOTE: Before you can delete a GoS quality group, you must delete all security policies that refer to the quality group. To list all security *policies, enter the command* **show security policy**. *Look for the quality group name in the* **QoS** *field.*

The following example deletes the quality group named Data:

```
> del qos group Data
*> save
```

Assigning Traffic Flows to Quality Groups

This section describes how to assign outgoing traffic flows to GoS quality groups.

When outgoing traffic is assigned to a quality group, its quality treatment is determined by the settings for that group. If traffic is not matched to a quality group, it is managed by the default quality group assigned to BE (best effort).

NOTE: A quality group must be configured before it can be referenced by a command.

Usually, a traffic flow is assigned to a quality group using a security policy. However, quality groups for VoIP and ARP traffic are specified on separate commands, as described in the following sections.

VoIP Traffic Protection

To protect VoIP traffic, two quality group settings are needed: one to protect VoIP signaling traffic and the other to protect VoIP media streams.

The quality group to protect VoIP signaling traffic is specified by the **sigqos** parameter. Enter it as a session controller setting (see "Session Controller Setting Command" (page 272) [SIP] or in "Session Controller Setting Command" (page 216) [MGCP]).

For example, assume that a quality group named *VoIPSignaling* is configured to protect signaling traffic. To specify the quality group as a SIP session controller setting, enter:

```
> config sip sc setting sigqos VoIPSignaling
```

To specify the quality group as a MGCP session controller setting, enter:

```
> config mgcp sc setting sigqos VoIPSignaling
```

The quality group to protect VoIP media streams is specified by the **audioqos** parameter. Enter it as a media setting. (The media setting is independent of the signaling protocol, SIP or MGCP; see "Media Settings Command" (page 229)).

For example, assume that a quality group named *VoIPMedia* is configured to protect media streams. To specify the quality group as a media setting, enter:

```
> config media setting audioqos VoIPMedia
```

ARP Traffic Protection

A special command is provided to assign ARP traffic to a GoS quality group. (The ARP traffic flow cannot be classified by a security policy because it does not go through the firewall. For further information, see "ARP Traffic Protection Example" (page 124)).

To protect ARP traffic, specify the name of the appropriate GoS quality group on the following command:

```
> config protocol arp qg
```

Ensure that the quality group assigned to protect ARP traffic is a group that ensures low packet loss and uses strict policing. The group should not allow ARP packets to be treated as best effort (BE) traffic (see "Quality Groups" (page 182)). For an example, see "ARP Traffic Protection Example" (page 124).

Traffic Protection by Security Policy

A security policy defines an outgoing traffic flow and specifies the GoS quality group to protect that traffic flow. The maximum number of GoS policies (and protected traffic flows) is 50.

To configure a security policy, enter the following command:

```
> config security policy
```

Table 41 describes the parameters for **config security policy**. Use the same command to define security policies for the firewall, NAT, and GoS. For GoS, the security policy parameters are used as follows:

- The **qosqg** parameter specifies the GoS quality group to which the traffic flow is assigned.
- The following parameters define the traffic flow. Specify only those parameters required to define the flow. Every value specified must match the corresponding packet value:
  - Interfaces (**from**, **to**)
  - IP addresses (**srcip**, **destip**)
  - Port numbers (**sport**, **dport**)
  - Protocol (**proto**)
  - IPToS tag value (**iptos**)
- A packet is compared to each policy in sequential order until a match is found. The policy order is determined by the **index** and **seq** parameters.
- The **nat** parameter does not affect GoS processing.
- The **action** parameter must **allow**, not **deny**, packets (the default value). Denied traffic is discarded and not processed by GoS.

GoS Security Policy Examples

The following examples illustrate the configuration of security policies to define GoS traffic flows.

Example 1

This example assumes that a GoS quality group named Data is configured. The security policy defines the FTP traffic flow to be protected by the Data quality group. The traffic flow consists of all TCP packets sent from LAN IP address 10.0.1.100 to WAN IP address 192.168.134.100 with destination port 20 or 21.

```
> config security policy new from eth1 to eth0 srcip
10.0.1.100 destip 192.168.134.100 proto tcp dport 20-21 qosqg
Data
*> save
```

Example 2

This example assumes that a GoS quality group named Data is configured. The security policy defines a traffic flow to be protected by the Data quality group. The traffic flow consists of all SNMP traffic sent from the unit to the WAN IP address 192.168.134.101. SNMP traffic is defined as UDP traffic from source port 161.

```
> config security policy new from self to eth0 sport 161
destip 192.168.134.101 proto udp qosqg Data
*> save
```

Show GoS Security Policies

The command to show the GoS security policies is the same as the one to show other security policies, as follows:

```
> show security policy
```

The GoS security policies are the policies listed with a value in the QoS field:

```
Security Policies:

Id Seq From  Source IP    Dest IP          Source Dest  Proto  NAT QoS
       To                                              Action ToS
-------------------------------------------------------------------
1  1   eth1  10.0.1.100   192.168.134.100  any    20-21  tcp    0  Data
       eth0                                             allow  any
2  1   self  any          192.168.134.101  161    any    udp    0  Data
       eth0                                             allow  any
```

Delete a Security Policy

To delete a security policy, specify its Id on the command **del security policy**.

For example, the following command deletes security policy **1**:

```
> del security policy 1
*> save
```

GoS Statistics

Two types of GoS statistics are available:

- **Cumulative statistics**: packet and byte counters incremented until the counters are cleared.
- **Instantaneous statistics**: rates calculated over a one-second interval.

Cumulative Statistics

Cumulative statistics are recorded both for each quality group and for all best effort (BE) traffic for the link.

Best Effort Statistics

To display cumulative statistics for all best effort (BE) traffic on the link, specify the link on the command **stats qos link**. For example, to display the BE statistics for eth0, enter:

```
> stats qos link eth0

Link           eth0

Packets in     159161356
Packets out    159161356
Packets dropped0
Bytes in       209556913319 bytes
```

```
Bytes out       209556913319 bytes
Bytes dropped   0 bytes
```

Quality Group Statistics

To display cumulative statistics for a quality group, specify the group name on the command **stats qos counters**.

For example, to display the cumulative statistics for the quality group VoIP, enter:

```
> stats qos counters VoIP
Name                        VoIP
Link                        eth0

 Packets in:                2572
 Primary packets out:       2572
 Downgraded packets:        0
 Packets dropped:           0
 Bytes in:                  278950 bytes
 Primary bytes out:         278950 bytes
 Bytes dropped:             0 bytes
 Bytes downgraded:          0 bytes
```

As listed in Table 66, statistics are displayed for both packet counts and byte counts. Byte counts include the Ethernet header without FCS for an Ethernet link.

Table 66. GoS Cumulative Statistics

Counter	Description
Packets in	Total number of packets received; the number of packets offered to the quality group.
Primary packets out	Total number of packets forwards on the primary output. The quality group protects and forwarded these packets because they arrive within the committed rate.
Downgraded packets	Total number of packets downgraded. The quality group forwards these packets to the best effort quality group. This counter applies only to quality groups that use CAR policing, as the group represents packets that arrive above the committed rate, but below the burst rate.
Packets dropped	Total number of packets dropped: - If the quality group uses strict policing, the packets are dropped because they arrive at a rate over the committed rate. - If the quality group uses CAR policing, the packets are dropped because they arrive at a rate over the burst rate.
Bytes in	Byte count for the **Packets in** counter.
Primary bytes out	Byte count for the **Primary packets out** counter.

Table 66. GoS Cumulative Statistics (continued)

Counter	Description
Bytes dropped	Byte count for the **Packets dropped** counter.
Bytes downgraded	Byte count for the **Downgraded packets** counter. This statistic is not provided for best effort traffic.

Clearing GoS Cumulative Statistics

As needed, you can clear the GoS statistic counters and reset to zero.

Best Effort Statistics

To clear the BE statistics kept for the link, specify the link on a **clear qos link** command.

For example, this command clears the BE statistics for the eth0 link:

```
> clear qos link eth0
```

Quality Group Statistics

To clear the statistics kept for a quality group, specify the quality group on a **clear qos counters** command.

For example, the following command clears the statistics for quality group VoIP:

```
> clear qos counters VoIP
```

To clear the GoS statistics of all quality groups, enter the following command:

```
> clear qos counters all
```

Instantaneous Statistics

Instantaneous statistics are available to show the current GoS rates, calculated over a one-second interval.

To display instantaneous statistics for a quality group, specify the group name on the command **stats qos group**.

For example, to display the instantaneous statistics for the quality group VoIP, enter:

```
> stats qos group VoIP
Name                          VoIP
Link                          eth0

 Input rate:                  142525 bps
 Output rate:                 142525 bps
 Primary output rate:         142525 bps
 Downgrade output rate:       0 bps
 Packet loss rate:            0 pps
 Data loss rate:              0 bps
 Packet loss ratio:           0 percent packets lost
 Data loss ratio:             0 percent bytes lost
 Average packet size:         152.27 bytes
```

Table 67 describes the statistics of **stats qos group.** Byte counts include the Ethernet header without FCS for an Ethernet link.

Table 67. GoS Instantaneous Statistics

Statistic	Description
Input rate	Offered rate to the quality group.
Output rate	Overall output rate of the quality group, including protected and downgraded traffic.
Primary output rate	Output rate of the protected traffic.
Downgrade output rate	Output rate of downgraded (nonprotected) traffic. This rate applies only to quality groups that use CAR.
Packet loss rate	Rate of packets dropped by the quality group: - If the quality group uses strict policing, the packets are dropped because they arrive at a rate over the committed rate. - If the quality group uses CAR policing, the packets are dropped because they arrive at a rate over the burst rate.
Data loss rate	**Packet loss rate** translated to bytes per second.
Packet loss ratio	Ratio comparing total packets out to total packets in.
Data loss ratio	Ratio comparing total bytes out to total bytes in.
Average packet size	Average packet size in bytes.

Configuring QoS

This section describes the steps for setting up QoS in order to protect VoIP traffic from Data traffic.

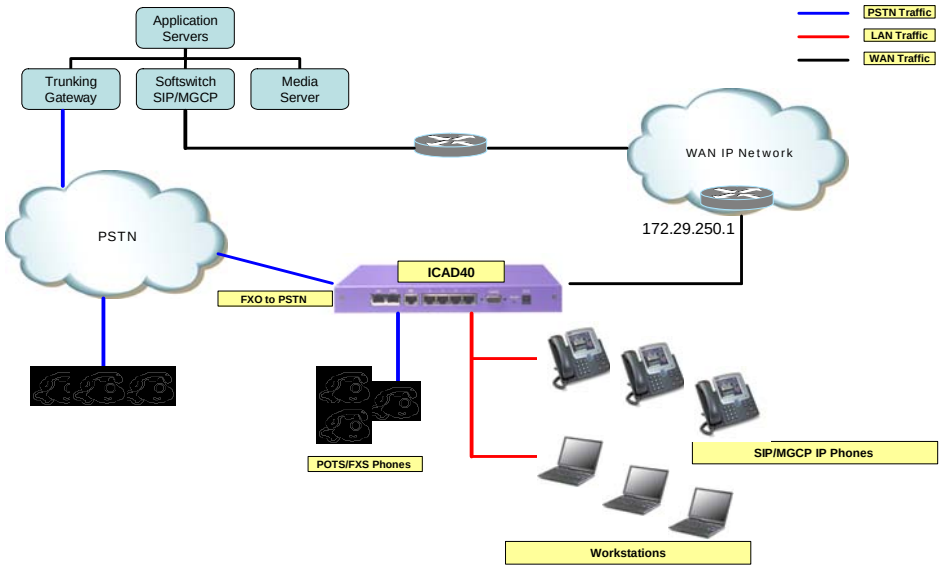


Table 68 describes network information, and Table 69 describes server information

Table 68. Network Information

LAN IP range Access router	10.0.0.0/16 10.0.1.1 (BSGX4e)
WAN range Access router	172.29.0.0/16 172.29.250.1

Table 69. Server Information

S1 DHCP Server	dhcpserver.isp.com - 66.19.9.160 (the access router acting as a DHCP relay between the BSGX4e and the DHCP server)
S2 HTTP Server	Httpserver.isp.com - 66.19.9.161
S3 SIP Server	Sipserver.com - 66.19.9.162 / SIP domain "sip.net"
S4 NTP Server	ttpserver.isp.com - 66.19.9.163
S5 TFTP Proxy	tftpserver.isp.com - 66.19.9.164
S6 DNS Server	dnsserver.isp.com - 66.19.9.165

Configuration guidelines describe an actual case for configuring an BSGX4e for deployment at a small customer office to implement a complete Voice over Internet Protocol (VoIP) (SIP environment) and data solution:

- The SIP Session Controller (SIP SC) controls VoIP telephones installed in the Local Area Network (LAN). The SIP User Agent (SIP UA) controls the analog fax machine attached to the FXS port of the BSGX4e.
- Workstations installed in the LAN access various data services such as e-mail, chat, and the World Wide Web.
- VoIP traffic is protected from data traffic.

To configure the Quality of Service of the BSGX4e, you must understand how VoIP and data flows go through the BSGX4e.

Figure 12 shows the logical path of flows

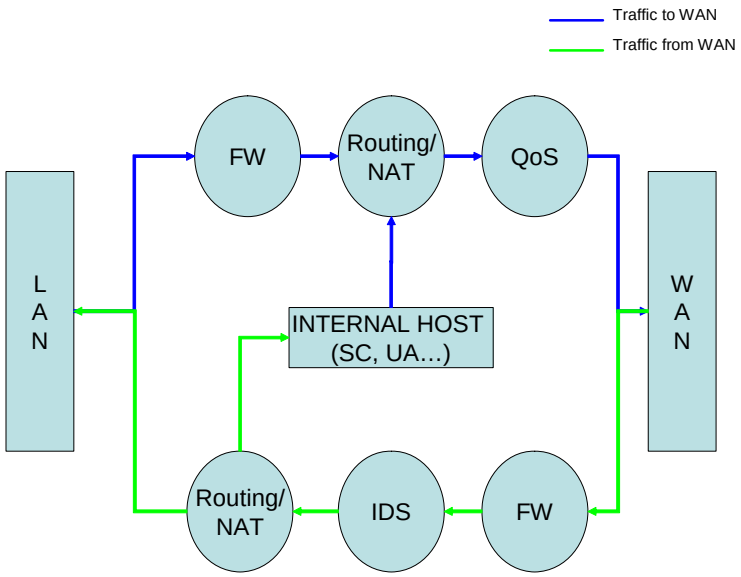


Figure 12. Logical path

Flows are exchanged between three components: equipment located in LAN, equipment located in Wide Area Network (WAN), and the internal host handling services such as the Session Controller and the User Agent.

Traffic from the LAN goes through the Firewall (FW), Routing/NAT, and Quality of Service (QoS). Traffic from the WAN goes through the Firewall, Intrusion Detection System (IDS), and Routing/NAT. Traffic to the WAN is trusted so it does not need to be checked by the Intrusion Detection System. Traffic from the WAN usually has a low speed, so you do not need QoS. Figure 13 shows the hardware path of flows.

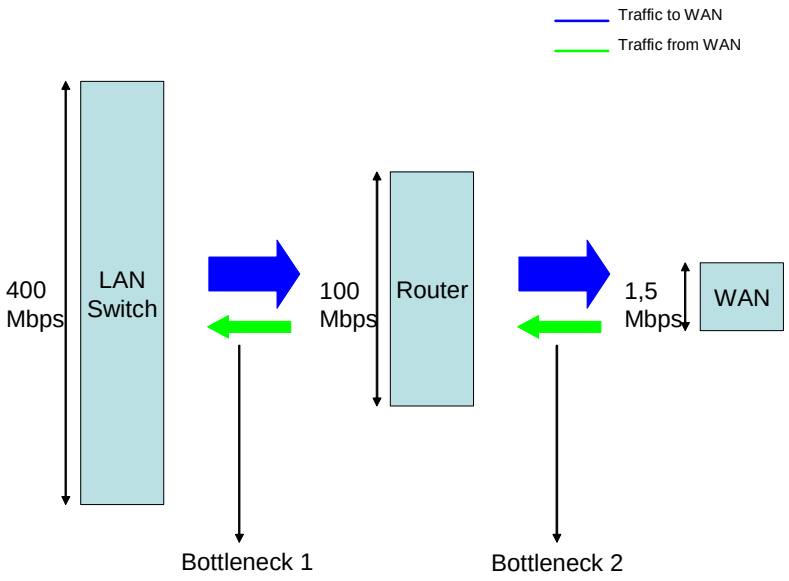


Figure 13. Hardware path

Traffic to the WAN suffers from two bottlenecks. The first one concerns the LAN-switched traffic sent to be forwarded to the WAN. The uplink of the four-port LAN switch to the router runs at 100 Mbps (in reality the switch has five ports; four are in the rear of the BSGX4e and one is internally connected to the routing engine). The first bottleneck is to handle a theoretical 400 Mbps offered load to forward to a 100 Mbps uplink. The Layer 2 QoS feature of the BSGX4e manages this bottleneck. The second bottleneck concerns the routed traffic that is sent to the WAN. Up to 100 Mbps can be received from the LAN, and the internal host can also need to send traffic to the WAN (such as VoIP traffic when the SIP UA is running). Therefore the second bottleneck handles a theoretical 100+ Mbps offered load to forward to a low speed WAN link such as T1 (1.5 Mbps). The Layer 3 QoS feature of the BSGX4e manages the second bottleneck.

The QoS solution of the BSGX4e includes two QoS mechanisms, one is operating at Layer 2, the other is operating at Layer 3.

The LAN switch runs Layer 2 QoS. The classification is based on the ingress port identifier, DSCP/ToS byte or IEEE 801.p tag. Each port implements four priority queues. You do not need to do any bandwidth calculations. It is especially useful to run the ones of the uplink port (the port sending packets to the routing engine). You can choose to run a strict priority queuing or a weighted fair queuing mechanism. The worst scenario is to have the four rear ports receiving 100 Mbps, switched to the uplink in order to be routed to the WAN.

The routing engine runs Layer 3 QoS. Guarantee of Service (GoS) is implemented. For more information about GoS, see the GoS documents. GoS allows applying or controlling three QoS constraints per traffic type: bandwidth, loss and delay. Bandwidth calculations take into account the Ethernet header size (14 bytes), because packets are transmitted to the WAN over the Ethernet. Loss and delay are defined relatively among traffic types. The classification is based on Layer 3/4 information such as IP address, IP Terms of Service (ToS), or User Datagram Protocol (UDP)/Transmission Control Protocol (TCP) port. The WAN port of the BSGX4e implements the GoS queuing mechanism made of policers, shapers, and multiplexers. GoS is not yet implemented to control the traffic on the LAN port (coming from the host or WAN). The worst scenario is to have 100 Mbps of traffic coming from the LAN plus a small amount of traffic coming from the host (such as VoIP traffic when the SIP UA is running) to be routed to a very low speed link such as a 128 Kbps Integrated Services Digital Network (ISDN) line or similar.

Example

The following example shows how to deploy QoS to protect VoIP and management traffic.

Analyze

Traffic management requires that you first analyze the flows going through the BSGX4e. In this example assume you want to manage the following traffic types for a T1 WAN link (in other words, a Full T1 modem is located behind the BSGX4e):

- VoIP (signalling and media): 44 G.729a calls between LAN and WAN + 1 G.711u call between the host (UA) and WAN (this is typically the case of a fax connected to the FxS port of the BSGX4e).
- Management: SNMP polling between the host and WAN (this is typically the case of a network management workstation located on the ISP side).
- Other: Various traffic types such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Domain Names Service (DNS), or Network Time Protocol (NTP).

Traffic management requires then defining which QoS constrains (bandwidth, loss, delay) to apply to each of these traffic types:

- VoIP (signalling): VoIP signalling does not require a very high bandwidth, 64 Kbps is enough. SNMP traffic is very sensitive to loss but less to delay. By assigning to this traffic a bandwidth of 64 Kbps, you ensure no signalling packets will be dropped.
- VoIP (media): Because the WAN interface of the BSGX4e is Ethernet, all bandwidth calculations take into account the Ethernet header (14 bytes) + IP header (20 bytes) + IP payload. They do not take into account Ethernet FCS. One G.729a call is a flow of 50 pps of 74-byte packets (including the Ethernet header). One G.711u call is a flow of 50 pps of 214-byte packets (including the Ethernet header). Therefore the bandwidth required for VoIP flows is (44 x 50 x 8 x 74) + (1 x 50 x 8 x 214) = 1 388 000 bps. You can assume here that endpoints do not send RTCP traffic; otherwise you can plan a slightly higher rate. Loss and delay for real-time traffic must be as low as possible.

- Management: SNMP polling does not require a very high bandwidth, 64 Kbps is enough. SNMP traffic is not very sensitive to loss and delay. By assigning to this traffic a bandwidth of 64 Kbps you can ensure too many packets are not dropped (the rate can be higher at some times) so the SNMP applications can run normally (no timeout).
- Other: The other traffic can be handled in best effort mode, for which no bandwidth is allocated and nothing is required for the loss and delay.

Traffic management requires defining how to classify the traffic to distinguish the different traffic types:

- VoIP (signalling and media): Because the SIP Session Controller controls the VoIP calls established through the BSGX4e, it knows which packets (signalling and media) belong to VoIP traffic type.
- Management: Assuming the SNMP agent is configured to listen and transmit SNMP packets on port 161, this traffic type can be classified based on port (161) and protocol (UDP).
- Other: You do not need to specify any classification rules for the other flows. By default, flows are managed in best effort.

To conclude the analysis, you must define the bandwidth of the WAN T1 link. This determines at which speed the routing engine can transmit packets from its WAN interface. A T1 interface usually runs at 1.536 Mbps (taking into account the Frame Relay header and Frame Check Sequence (FCS)). IP packets sent to the T1 link have a Frame Relay overhead of 6 bytes in the case Data Link Connection Identifiers (DLCI) are coded on 10 bits (four for the overhead and two for FCS) while packets sent by the BSGX4e have a Ethernet overhead of 14 bytes. This means you can configure the bandwidth of the Layer 3 QoS to a value greater than 1.536 Mbps, but not too much to avoid overwhelming the T1 link. By experience, the value 1 684 450 Mbps is good.

Configuring Layer 2 QoS

The configuration of Layer 2 QoS requires the following steps:

1. Configuring the classification type.
   Assume all VoIP signalling and media packets are tagged with a DiffServ/ToS byte of 45.

```
BSG> config switch qos setting type ToSDiff
```

2. Configuring the queuing mechanism.
   Strict priority and weighted round robin queuing mechanisms are supported. Because real-time traffic such as VoIP is sensitive to packet loss and delay, strict priority queuing is recommended.

```
*BSG*> config switch qos setting scheduling fixed
 *BSG*> show switch qos setting
Switch QoS:

Type Scheduling
--------------------------
TOS* FIXED
```

3. Configuring the mapping between the DiffServ/ToS byte value and the priority queue (classifier).
   VoIP packets are tagged with a DiffServ/ToS byte of 45.

```
*BSG*> config switch qos tos 45 priority highestq
*BSG*> show switch qos tos
Switch QoS:
TOSDiff Priority
---------------------------
0       LOWESTQ
1       LOWESTQ
2       LOWESTQ
3       LOWESTQ
4       LOWESTQ
5       LOWESTQ
6       LOWESTQ
7       LOWESTQ
8       LOWESTQ
9       LOWESTQ
10      LOWESTQ
11      LOWESTQ
12      LOWESTQ
13      LOWESTQ
14      LOWESTQ
15      LOWESTQ
16      LOWESTQ
17      LOWESTQ
18      LOWQ
19      LOWESTQ
20      LOWQ
21      LOWESTQ
22      LOWQ
23      LOWESTQ
24      LOWESTQ
25      LOWESTQ
26      HIGHQ
27      LOWESTQ
28      HIGHQ
29      LOWESTQ
30      HIGHQ
31      LOWESTQ
32      LOWESTQ
33      LOWESTQ
34      HIGHQ
35      LOWESTQ
36      HIGHQ
37      LOWESTQ
```

```
38      HIGHQ
39      LOWESTQ
40      LOWESTQ
41      LOWESTQ
42      LOWESTQ
43      LOWESTQ
44      LOWESTQ
45      HIGHESTQ
46      HIGHESTQ
47      LOWESTQ
48      LOWESTQ
49      LOWESTQ
50      LOWESTQ
51      LOWESTQ
52      LOWESTQ
53      LOWESTQ
54      LOWESTQ
55      LOWESTQ
56      LOWESTQ
57      LOWESTQ
58      LOWESTQ
59      LOWESTQ
60      LOWESTQ
61      LOWESTQ
62      LOWESTQ
63      LOWESTQ
```

4. Layer 2 QoS is now configured. Check that Layer 2 QoS is working correctly. The offered load of traffic to be sent to the routing engine through the uplink port is greater than 100 Mbps, some of the incoming packets on the four front ports is discarded. This is reported by the counter InDiscards on each of the four ports. Example for port 1:

```
*BSG*> stats switch port 1
Port "0-1" stats:

Tx                12154786              Rx                12277665
OutUnicasts       12137156              In Unicasts       12277269
OutBroadcasts        14980              InBroadcasts      396
OutPause                 0              InPause           0
OutMulticasts         2650              InMulticasts      0
OutFCSErr                0              InFCSErr          0
Out64Octets          32842              In 64 Octets      36930
Out127Octets      11994789              In127Octets       12222457
Out255Octets         99459              In255Octets       0
Out511Octets          9179              In511Octets       9139
Out1023Octets        18517              In1023Octets      9139
OutMaxOctets             0              InMaxOctets       0
```

```
Deferred                  0              InDiscards          879
Out Octets        978710557              InGoodOctets        968946799
AlignErr                  0              InBadOctets         0
Oversize                  0              Undersize           0
Jabber                    0              Fragments           0
Collisions                0              Late Collisions     0
Excessive                 0              Filtered            0
Single                    0              Multiple            0
```

Configuring Layer 3 QoS

The configuration of Layer 3 QoS requires the following steps:

1. Configuring the size of the WAN link.
   You can manage the traffic for a full T1 WAN link.

```
*BSG*> config qos link eth0 max 1684450 comment "Full T1 WAN link"
*BSG*> show qos link
QoS Links:

Interface Max             Comment
---------------------------------------------
eth0      1684450         Full T1 WAN link
```

2. Configuring QoS Quality Groups (QoS constraints).
   QoS constraints for VoIP signalling traffic are bandwidth: 64 000 bps, low loss and medium delay (Class of Service A2). Also, you can use a CAR policer to allow bursts if there is free bandwidth.

```
*BSG*> config qos group VoIP_sig qg a2 type car committed 64000 burst
       1000000
```

   QoS constraints for VoIP media traffic are bandwidth: 1 388 000 bps, low loss and low delay (Class of Service A1). Also, you can use a POLICED policer to guarantee the entire offered load.

```
*BSG*> config qos group VoIP_med qg a1 type policed committed 1388000
```

   QoS constraints for Management traffic are bandwidth: 64 000 bps, medium loss and medium delay (Class of Service B2). Also, a CAR policer is used in order to allow bursts if there is free bandwidth.

```
*BSG*> config qos group Management qg b2 type car committed 64000 burst
       1000000
*BSG*> show qos group
QoS Quality Groups:
Name            Link  QG    Type       Committed  Burst      IPToS COS
-------------------------------------------------------------------------
Management      eth0  B2    car        64000      1000000    no    no
VoIP_med        eth0  A1    policed    1388000    0          no    no
VoIP_sig        eth0  A2    car        64000      1000000    no    no
```

7. Configuring the classifier.

The SIP Session Controller detects VoIP signalling packets. You must configure it to manage them by the QoS Quality Group VoIP_sig.

```
*BSG*> conf sip sc settings sigqos VoIP_sig
*BSG*> show sip sc settings
SIP Session Controller settings:

   Server     SipProxy
   Local Domain
   Wan Rx Port             5060
   Lan Rx Port             5060
   Timer T1                500 msec
   Timer T2                4000 msec
   Timer B                 16 sec
   Timer F                 32 sec
   Timer C                 180 sec
   Max Calls               500
   Signaling QoS Group     VoIP_sig
```

The SIP Session Controller detects VoIP media packets. You must configure it to manage them by the QoS Quality Group VoIP_med.

```
*BSG*> conf media settings audioqos VoIP_med
*BSG*> show media settings
Media config:

   Direct Media Enabled     No
   RTP Ports                13000 - 14999
   AudioQoS                 VoIP_med
   MaxConn                  500
```

You must classify management packets manually to be managed by the QoS Quality Group Management.

```
*BSG*> conf security policy new from self to eth0 sport 161 proto udp
       qosqg Management
*BSG*> show security policies
Security Policies:
```

```
Id Seq From  Source IP        Dest IP          Source Dest  Proto  NAT QoS
      To                                                    Action ToS
-------------------------------------------------------------------------------
1  1   eth0  any              any              any    any   any    0
       self                                                 allow  any
2  3   eth0  172.29.3.191     any              any    any   esp    0
       self                                                 allow  any
3  5   eth0  any              any              any    22    tcp    0
       self                                                 allow  any
4  7   eth0  any              any              any    443   tcp    0
       self                                                 allow  any
5  9   eth0  any              any              any    80    tcp    0
       self                                                 allow  any
6  11  eth0  any              any              any    23    tcp    0
       self                                                 allow  any
7  1   eth0  any              any              any    any   any    0
       eth1                                                 allow  any
8  1   eth1  any              any              any    any   any    0
       eth0                                                 allow  any
9  1   eth1  any              any              any    any   any    0
       self                                                 allow  any
10 1   eth1  any              any              any    any   any    0
       vpn0                                                 allow  any
20 1   self  any              any              161    any   udp    0   Mana*
       eth0                                                 allow  any
```

8. Layer 3 QoS is now configured. Check that Layer 3 QoS is working correctly. When a call is established through the BSGX4e, the QoS counters can be incremented for both Quality Groups VoIP_sig and VoIP_med. You must never observe any packets dropped for VoIP_med (because VoIP traffic is protected). If packets are dropped for VoIP_med, the offered load exceeds 1 388 000 bps, so there is likely something wrong in the setup of the network. Also, you must never observe any packets downgraded, because VoIP_med uses a POLICED policer. You may observe downgraded packets for VoIP_sig, because it uses a CAR policer (if the offered load is higher than 64 Kbps, it is downgraded in best effort), but this is unlikely.

```
*BSG*> stats qos counter VoIP_sig
 Name                    VoIP_sig
 Link                    eth0

 Packets in              1036
 Packets out             1036
 Downgraded packets      0
 Packets dropped         0
 Bytes in                663544 bytes
 Bytes out               663544 bytes
 Bytes dropped           0 bytes
 Bytes downgraded        0 bytes

*BSG*> stats qos counter VoIP_med
 Name                    VoIP_med
 Link                    eth0
```

```
 Packets in             2211704
 Packets out            2211704
 Downgraded packets     0
 Packets dropped        0
 Bytes in               406953536 bytes
 Bytes out              406953536 bytes
 Bytes dropped          0 bytes
 Bytes downgraded       0 bytes
```

When the BSGX4e is polled by a SNMP network management workstation, the QoS counters can be incremented. You may observe downgraded packets because the Quality Group Management uses a CAR policer (if the offered load is higher than 64 Kbps, it is downgraded in best effort). You may observe dropped packets if the offered load exceeds the burst rate (1 000 000 bps), but this is unlikely.

```
*BSG*> stats qos counter Management
 Name                    Management
 Link                    eth0

 Packets in             1265
 Packets out            1265
 Downgraded packets     0
 Packets dropped        0
 Bytes in               806566 bytes
 Bytes out              806566 bytes
 Bytes dropped          0 bytes
 Bytes downgraded       0 bytes
```

When other traffic types run, they are managed in best effort mode. It is likely to have packets dropped, showing that low priority packets have been discarded by the QoS mechanism because the offered load has been greater than the QoS link rate (1 684 450 bps).

```
*BSG*> stats qos link eth0
Link                 eth0

 Packets in          6217
 Packets out         6217
 Packets dropped     45
 Bytes in            1403973 bytes
 Bytes out           1403973 bytes
 Bytes dropped       5684 bytes
```

12 MGCP CONFIGURATION

This chapter describes the configuration of the MGCP session controller and the integrated MGCP gateway. You can configure the BSGX4e device to act as both VoIP session controller and VoIP gateway. The session controller and VoIP gateway can use either the Session Initiation Protocol (SIP) or the Media Gateway Control Protocol (MGCP).

Configuration for SIP is described in "SIP Configuration" (page 263). VoIP topics that apply to both signaling protocols (SIP and MGCP) are discussed in "VoIP Configuration" (page 229).

Introduction to MGCP

The Media Gateway Control Protocol (MGCP) session controller controls the establishment and termination of VoIP sessions, as requested by endpoint devices. The MGCP gateway, which operates together with the session controller, serves as the VoIP gateway for a Private Branch Exchange (PABX) or other analog devices.

Figure 14 shows an MGCP network. In the figure, the BSGX4e device controls VoIP sessions for its LAN devices, which can be MGCP phones and PC terminals. The BSGX4e device can also control VoIP sessions for an analog device (fax machine or phone) connected to its FXS port. To do so, the BSGX4e unit requires access through the WAN to one or more MGCP servers.

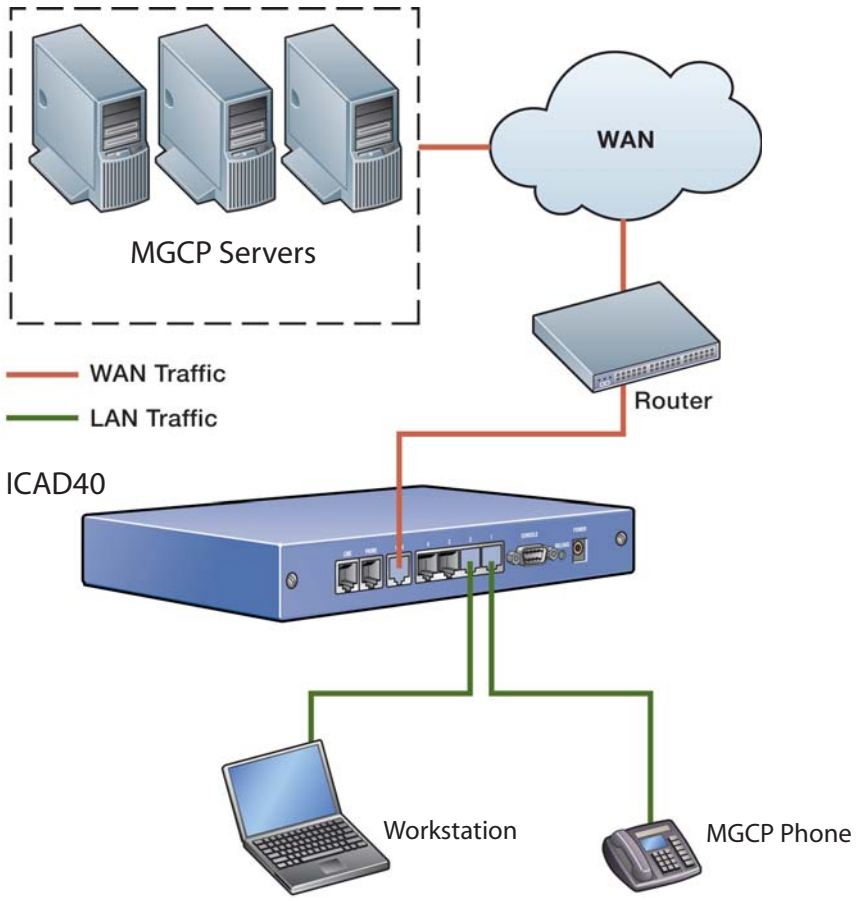


Figure 14. MGCP Network Layout

MGCP Session Controller

All VoIP traffic is directed through the session controller, allowing the session controller to isolate and control all VoIP devices on the internal network (LAN). The session controller can handle up to 1000 VoIP endpoints and up to 500 concurrent calls.

The session controller provides the following services:

- Serves as the interface between MGCP endpoints and the MGCP call server on the WAN. It interprets and relays all messages between the call server and the MGCP devices on the LAN.
- Modifies Session Description Protocol (SDP) information to accommodate direct media connections and bridged connections (from LAN endpoint to LAN endpoint and from LAN endpoint to an endpoint on the WAN). This service is described in "Media Bridge (MBR)" (page 229).
- Performs the following *Keep-alive* functions:
  - If the call server should not receive *Keep-alive* messages, the session controller filters them out.

- If the call server requires *Keep-alive* messages, but a LAN endpoint device does not send those messages, the session controller generates those packets for the endpoint device.

- Tracks device status on the LAN to learn when a LAN endpoint goes down (using Audit Endpoint (AUEP) requests). The MGCP registration information is kept in nonvolatile storage, so it can be immediately restored at restart.
- Manages the Access List Control (ACL) rules. Registration and call requests are accepted or rejected as directed by ACL rules. See "Access Control List (ACL)" (page 232).
- Rejects call requests if the endpoint is not registered (RSIP).
- Rejects call requests if bandwidth is not available for the call. See "Call Admission Control (CAC)" (page 236).
- Monitors voice quality. See "Voice Quality Monitoring (VQM)" (page 247).
- Supports *local call routing*: when VoIP service is unavailable, the MGCP session controller still routes local calls within the LAN. It can also, optionally, route external calls to the PSTN network. See "Local Call Routing" (page 255).

MGCP Gateway

The FXS port of the BSGX4e device can provide VoIP communication capabilities for an analog device. To do so, you must configure the integrated MGCP gateway (also known as the MGCP user agent). The MGCP gateway interfaces VoIP to POTS and connects an analog device (PABX, phone, modem, or fax machine) to the MGCP network.

MGCP Gateway Features

The MGCP gateway supports the following features:

- Functions as an MGCP integrated access device (IAD).
- Works with the digit maps of the call server to initiate calls as soon as enough digits are received from the analog interface, instead of waiting for timeout.
- Supports analog telephone features. (The MGCP gateway detects hook flash in FXS and reports the event to the call agent.) The features include:
  - Call on hold / retrieve
  - Place or receive a second call
  - Call transfer
  - Three-way conferencing
  - Call waiting notification

MGCP Configuration Steps

The MGCP configuration steps are:

1. **Configure access to one or more MGCP servers.**
2. **Configure the MGCP session controller.**
3. **Configure MGCP telephones, including the MGCP gateway.**

MGCP Call Servers

This section describes how to configure a server profile, which determines how the session controller accesses MGCP servers to provide VoIP service. An MGCP server is also known as a Media Gateway Controller (MGC).

One of the session controller settings specifies the call server profile that the session controller is to use. A server profile can explicitly specify up to three MGCP servers. The MGCP session controller can only locate MGCP servers that are explicitly specified; MGCP servers cannot be located through DNS.

NOTE: The firewall is automatically updated to accept MGCP messages from each configured MGCP server.

Call Server Failover

Call server failover prevents VoIP service interruption by providing backup call servers. Call server failover is available only if the server profile used by the session controller explicitly specifies more than one MGCP server. Then, if the current MGCP server becomes unavailable, the session controller can reference the next MGCP server in the profile.

When the server profile specifies only one server, the MGCP session controller communicates only with that MGCP server. If that server becomes unavailable, the MGCP session controller continuously retries to contact it. No calls can be established until the *mgc1* server recovers.

When failover is available, the MGCP session controller detects that the MGCP server is unavailable either when the server has no IP connectivity with it or when the server receives no MGCP replies from it. When this happens, the MGCP session controller:

- Marks the MGCP server as down for the duration configured by the *blacklist* parameter; the MGCP session controller does not try to contact the MGCP during the blacklist period.
- Attempts to communicate with the next MGCP server by priority.
- Tries to resume communication with the higher-priority server when its blacklist period expires.

The session controller detects that the call server might be down if it:

- cannot connect to it (for example, if the WAN interface is unplugged, or an IP route is not available)
- does not receive MGCP replies from it (The server profile specifies the number of retries.)

When the session controller detects that a server might be down, it attempts a number of retries before it marks the server as down. (The server profile specifies the number of retries.)

MGCP Server Profile Command

To configure an MGCP server profile, enter the following command:

```
> config mgcp server settings
```

Table 70 describes the parameters for **config mgcp server settings.**

Table 70. MGCP Server Profile Parameters

Parameter	Description
[name]	Name of the server profile to be created or edited.
mgc1	First Media Gateway Controller (either a fully qualified domain name [FQDN] or an IP address).
port1	Port number for *mgc1*. The default is **2727**.
mgc2	Optional second Media Gateway Controller (FQDN | IP address).
port2	Port number for *mgc2*. The default is **2727**.
mgc3	Optional third Media Gateway Controller (FQDN | IP address).
port3	Port number for *mgc3*. The default is **2727**.
retries	Number of retries before an MGC server is blacklisted. The default is **5** retries. (Specifying **0** disables call server failover.)
blacklist	Blacklist timer in seconds. The default is **600** seconds (ten minutes).

MGCP Server Profile Examples

The following examples configure two MGCP server profiles: one for a single MGC server and the other for two MGC servers. (The session controller setting determines which server profile is used.)

Single Server Example

This example configures a single MGC server:

Name of settings profile: Sylantro
IP address of MGC server: 206.229.26.51
Port number of MGC server: 2727

```
> config mgcp server settings Sylantro mgc1 206.229.26.51
port1 2727
*> save
```

Two Server Example

This example configures two MGC servers for failover mode:

Name of settings profile: Sylantro_FailOverMode
FQDN of higher-priority MGC server: primary.sylantro.com
Port number of higher-priority MGC server: 2727
FQDN of lower-priority MGC server: secondary.sylantro.com
Port number of lower-priority MGC server: 2727
Number of retries: 10

Blacklist duration: 300 seconds

```
> config mgcp server settings Sylantro_FailOverMode mgc1
primary.sylantro.com port1 2727 mgc2 secondary.sylantro.com
port2 2727 retries 10 blacklist 300
*> save
```

Show Server Settings

To show the MGCP server setting profiles, enter the following command:

```
> show mgcp server settings

MGCP Server "Sylantro":

   Name       Sylantro
   MGC1       206.229.26.51
   Port1      2727
   MGC2
   Port2      2727
   MGC3
   Port3      2727
   Retries    5
   Blacklist  600 sec

MGCP Server "Sylantro_FailOverMode":

   Name       Sylantro_FailOverMode
   MGC1       primary.sylantro.com
   Port1      2727
   MGC2       secondary.sylantro.com
   Port2      2727
   MGC3
   Port3      2727
   Retries    10
   Blacklist  300 sec
```

Delete MGCP Server Profile

To delete an MGCP server profile, specify its name on the command **del mgcp server settings**. For example, the following command deletes the profile *Sylantro*:

```
> del mgcp server settings Sylantro
```

Show MGCP Server Status

The session controller setting determines which server profile is used. (The profile name is specified by the *server* parameter on the **config mgcp sc settings** command.) To show the server profile currently in use, enter the following command:

```
> show mgcp server status
```

```
MGCP Server "Sylantro_FailOverMode":

   Name          Sylantro_FailOverMode
   Active        Yes
   MGC1          primary.sylantro.com (In-use)
   Port1         2727
   MGC2          secondary.sylantro.com (Ready)
   Port2         2727
   MGC3
   Port3         2727
```

The display shows the information specified by the setting. The display also shows the following status information:

Field	Description
Active	Yes This session controller is actively communicating with an MGCP server. No The session controller is not actively communicating with any server.
MGC1, MGC2, MGC3	(In-use) This server is currently in use. (Ready) This server is available, but is not currently in use. (Down) This server is not available.

MGCP Session Controller Configuration

The MGCP session controller provides the following features:

Feature	Description	Configuration Command
MGCP Signaling Proxy (MSP)	Relays MGCP messages between MGCP endpoints and MGCP servers	**config mgcp sc settings** (see "Session Controller Setting Command" (page 216)).
Media Bridge (MBR)	Controls how VoIP media traffic is established.	**config media settings** (see "Media Bridge (MBR)" (page 229)).
Access Control List (ACL)	Controls which LAN endpoints can place and receive calls.	**config voice acl** (see "Access Control List (ACL)" (page 232)).
Endpoint Status Handling (ESH)	Enables and disables LAN endpoints.	See "Endpoint Status Handling (ESH)" (page 220).
Call Admission Control (CAC)	Controls whether a call can be placed or received.	See "Call Admission Control (CAC)" (page 236).
Voice Quality Monitoring (VQM)	Reports the quality of calls.	**config calls analyzer** (see "Voice Quality Monitoring (VQM)" (page 247)).

MGCP Signaling Proxy (MSP)

The MGCP Signaling Proxy (MSP) relays MGCP messages between MGCP endpoints (phones or terminals) and a Media Control Gateway (MGC) server on the WAN.

The session controller settings are as follows:

- Modification information for MGCP headers so that messages can be relayed (`server`).

  Note: The MGCP session controller only supports the endpoint identification endpoint@domain-name in which the domain-name is a MAC address. It does not support identification per IP address.

- Ports on which to listen for MGCP signaling messages on the WAN and LAN, (`wanrxport` and `lanrxport` respectively).
- Indicator specifying that *Keep-alive* messages be sent to the MGCP server; this is used when the LAN endpoints do not send *Keep-alive* messages themselves (`keepalive`).
- GoS quality group to protect MGCP signaling from other traffic (`sigqos`). MGCP signaling traffic is sensitive to packet loss; if MGCP packets are dropped, calls can fail.

Configuration Prerequisites

Before a server profile can be specified for use by the session controller, the server profile must be configured (see "MGCP Call Servers" (page 212)).

To protect the quality of service for MGCP signaling traffic, a session controller setting assigns MGCP signaling traffic to a GoS quality group. You must configure the quality group before you can specify a session controller setting. For more information, see "GoS Configuration" (page 181).

Session Controller Setting Command

To configure the MGCP session controller, enter the following command:

```
> config mgcp sc settings
```

Table 71 describes the parameters for **`config mgcp sc settings`**.

Table 71. MGCP Session Controller Parameters

Parameter	Description
`server`	Name of the MGCP call server profile to be used. To see the configured server profiles, enter **show mgcp server settings**.
`wanrxport`	Port on which to listen for MGCP signaling messages from the WAN. The default is **2427**.
`lanrxport`	Port on which to listen for MGCP signaling messages from the LAN. The default is **2427**.
`keepalive`	Interval between keep-alive messages sent to the MGC server. Specify zero (**0**) to disable the sending of keep-alive messages. The default is **0**.

Table 71. MGCP Session Controller Parameters (continued)

Parameter	Description
eptimeout	Endpoint timeout interval (in seconds). The default is **3600** seconds (one hour). See "Endpoint Status Handling (ESH)" (page 220).
maxcalls	Maximum number of calls allowed simultaneously. The default is the maximum for the unit—**500** calls.
sigqos	Name of the GoS quality group that specifies the QoS protection for MGCP signaling traffic. To see the configured quality groups, enter **show qos group**.

MGCP Session Controller Setting Example

This example configures the MGCP session controller as follows:

Name of the MGCP server profile: Sylantro
WAN RX port: 2427
LAN RX port: 2427
GoS quality group to protect signaling traffic: VoIP

```
> config mgcp sc settings server Sylantro wanrxport 2427
lanrxport 2427 sigqos VoIP
*> save
```

Show Session Controller Settings

To show the session controller settings, enter the following command:

```
> show mgcp sc settings

MGCP Session Controller settings:

   Server                  Sylantro
   Wan Rx Port             2427
   Lan Rx Port             2427
   Keep Alive              0 sec
   EP Timeout              3600 sec
   Max Calls               500
   Signaling QoS Group     VoIP
```

Show MGCP Session Controller Status

To show the status of the MGCP session controller, enter the following command:

```
> show mgcp sc status

MGCP Session Controller status:

   MGC Started          Yes
   MGC Server Ready     Yes
```

```
My Wan IpAddr          192.168.134.217
Wan Rx Port            2427
Lan Rx Port            2427
CAC Max Calls          500
```

The display shows configured information and the following status field:

- `MGC Server Ready  Yes` if an MGCP server is active.
  `No` if no MGCP server is active.

Show MGCP Signaling Statistics

To show the counts for relayed MGCP signaling packets, enter the following command:

```
> stats mgcp sc status

MGCP Session Controller message stats:

   Msg per sec. (current/highest):      0/0

   TotalMsgRxCount                    200

   RxMsgDropSrcErr                      0
   RxMsgDropIntErr                      0
   RxMsgDropNoBufErr                    0
   RxMsgDropWanCsErr                    0
   RxMsgDropWanIfErr                    0
   TxMsgDropNoBufErr                    0
   TxMsgDropIntErr                      0

   WanMsgRecvCount                    100
   WanMsgProcCount                    100

   WanMsgDropDataErr                    0
   WanMsgDropNoBufErr                   0
   WanCmdCacRejErr                      0
   WanCmdDropSecFail                    0
   WanCmdDropDataErr                    0
   WanRspDropDataErr                    0
   WanRspDropStateErr                   0

   LanMsgRecvCount                    100
   LanMsgProcCount                    100

   LanMsgDropDataErr                    0
   LanMsgDropSecErr                     0
   LanMsgDropNoBufErr                   0
   LanCmdEacRejErr                      0
   LanCmdCacRejErr                      0
   LanCmdDropSecFail                    0
```

```
LanCmdDropDataErr                    0
LanRspDropDataErr                    0
LanRspDropStateErr                   0
```

The count fields (WanMsgRecvCount, WanMsgProcCount, LanMsgRecvCount, and LanMsgProcCount) report the counts of normal packets received and processed. The other fields report error counts.

The counters WanCmdCacRejErr and LanCmdCacRejErr report the number of calls rejected by Call Admission Control [see "Call Admission Control (CAC)" (page 236)].

Show MGCP Call Statistics

To show the statistics for MGCP calls, enter the following command:

```
> stats mgcp sc calls

MGCP Session Controller call stats:

  Call per sec. (current/highest):         0/0

  Active calls (current/highest):          0/0

  Total calls attempted:                   0

     Total outbound calls from LAN:        0
        Calls on going:                    0
        Calls succeeded:                   0
        Calls failed:                      0
        - Call rejected no bandwidth:      0
        - Call cancelled:                  0
        - Called dest busy:                0
        - Others causes:                   0

     Total inbound calls from WAN:         0
        Calls on going:                    0
        Calls succeeded:                   0
        Calls failed:                      0
        - Call rejected no bandwidth:      0
        - Call cancelled:                  0
        - Called dest busy:                0
        - Others causes:                   0
```

The first section, **Total outbound calls from LAN**, applies to calls that originate from LAN endpoints. The second section, **Total inbound calls from WAN**, applies to calls that originate from the MGCP server.

NOTE: A local call from a LAN endpoint to another LAN endpoint is shown twice in the statistics; it is counted as both a LAN outbound call and a WAN inbound call.

The counters **`Call rejected no bandwidth`** report the number of calls rejected by Call Admission Control [see "Call Admission Control (CAC)" (page 236)].

Show MGCP Call Records

The following command displays detailed information about MGCP calls:

```
  > show mgcp sc calls
MGCP Session Controller detailed call entries:

EP Call Info           Call to:  6019
   EP Info             4083747001@001122334455, 127.0.0.1:0
   Line Number         1
   Line State          CALL_CONNECTED
   Media Conn Mode     NORMAL
   Media Type          AUDIO
   Media Conn_b        66.206.164.199:32046--66.206.164.203:13024<==
   Media Conn_a              ==>127.0.0.1:13024--127.0.0.1:32100
```

Endpoint Status Handling (ESH)

The Endpoint Status Handling (ESH) saves information about LAN endpoints in nonvolatile memory, so the information can be retrieved after a restart. This information is saved during the MGCP registration process (RSIP). Information is stored about each LAN endpoint as it registers with the MGCP server.

The following information is stored:

- MGCP endpoint ID
- Name
- Telephone number
- IP address
- MGCP port
- MGCP call agent port
- Time remaining on the endpoint timer

The MGCP session controller rejects calls that terminate at endpoints not registered with the MGCP server. Because information about unregistered LAN endpoints is not stored, any unregistered endpoint is not reregistered when the unit restarts.

The session controller periodically checks the status of each LAN endpoint that uses the MGCP method AUEP. When a LAN endpoint answers, the endpoint timer (active time) is reset. If the endpoint does not answer, the MGCP session controller marks it as down and rejects all calls that terminate at that endpoint.

The only ESH value that can be configured is the value of the endpoint timer. The default timer value is 3600 seconds (one hour). You can change this value through the **eptimeout** parameter on the **config mgcp sc settings** command (see Table 71).

Changing the Endpoint Timeout

The following example specifies the server profile name (Sylantro) and changes the endpoint timer value to 1800 seconds:

```
> config mgcp sc settings server Sylantro eptimeout 1800
*> save
```

Show Endpoint Timer Value

To show the endpoint timer value, enter the following command:

```
> show mgcp sc settings
MGCP Session Controller settings:

   Server                  Sylantro
   Wan Rx Port             2427
   Lan Rx Port             2427
   Keep Alive              0 sec
   EP Timeout              1800 sec
   Max Calls               500
   Signaling QoS Group     VoIP
```

Show Registered Endpoints

The following command displays the list of LAN endpoints registered to the MGCP server through the MGCP session controller. This list is retrieved from memory when the unit restarts.

```
> show mgcp sc endpoints

MGCP Session Controller endpoints:

Endpoint ID               EP Addr      EP Port  Act Calls
Endpoint Name             TelNo        CA Port  Timeout
-----------------------------------------------------------
4083746017@00152b177677   10.0.1.57    2427     0
Sophia 6017               6017         2432     1500
4083747001@001111111111   127.0.0.1    0        0
                          7000         2429     1011
```

The configuration information in the display is stored when the endpoint is registered. In addition, the display shows the following status fields:

- CA Port

  Port to which call signals are sent; extracted from the last MGCP message received from the MGCP server, including a Notified Entity.

- Act Calls

  This field shows the currently active calls for the endpoint. The call count is incremented each time the LAN endpoint places or receives a call. The call count is decremented when the call is torn down.

- Timeout

This value represents the number of seconds before the registration expires. The initial value is taken from the **eptimeout** setting. The value is decremented each second.

MGCP Gateway

The integrated MGCP gateway (also known as the user agent) is the software in the BSGX4e device that allows an analog device such as a telephone or fax machine to use VoIP connections to place and receive calls. You must connect the analog device to the FXS port of the device as described in the installation guide.

This integrated MGCP gateway is configured as if it is a VoIP MGCP phone located on the LAN. MGCP identification (domain name) is supported by a MAC address only.

The MGCP gateway currently supports the following features:

- CODECs G.711 u-law, G.711 a-law and G.729
- RFC 2833
- Modem pass-through
- Fax pass-through
- Voice Activation Detection (VAD)

Configuration of the MGCP gateway requires the following steps:

1. Configure MGCP protocol settings for the gateway (see "Configuring MGCP Settings for the Gateway" (page 222)).
2. Configure FXS port settings (see "FXS Port Configuration" (page 238)).
3. Configure the MGCP gateway settings (see "Configuring the MGCP Gateway" (page 223)).

Configuring MGCP Settings for the Gateway

This section describes the MGCP protocol settings that apply to the MGCP gateway.

NOTE: The MGCP settings for the gateway do not apply to the MGCP session controller.

You can modify the MGCP protocol for interoperability purposes within the MGCP environment. The following changes can be applied to the MGCP protocol:

- domain format (currently, the only format supported is by MAC address)
- maximum number of retransmissions when a request does not receive an answer

NOTE: The MGCP protocol is configured so that the MGCP gateway tries to register with the MGCP server (using RSIP) as soon as the gateway is started. The MGCP gateway is not functional until it is registered.

MGCP Gateway Settings Command

To configure the MGCP protocol settings for the gateway, enter the following command:

```
> config mgcp ua settings
```

Table 72 describes the parameters for **config mgcp ua settings**.

Table 72. MGCP Gateway Parameters

Parameter	Description
domainformat	Format of MGCP endpoint domain names. Currently, the only format supported is by MAC address (**MACAddr**).
maxretxcount	Maximum number of successive retransmissions when a request does not receive an answer. The default is **5** retransmissions.

MGCP Gateway Settings Example

This example configures the MGCP settings for the gateway, as follows:

Domain format: MAC address
Maximum number of re-transmission: 5

```
> config mgcp ua settings domainformat MACAddr maxretxcount 5
*> save
```

Show MGCP Gateway Settings

To show the MGCP settings for the gateway, enter the following command:

```
> show mgcp ua settings
MGCP Protocol Settings:

   DomainFormat         MACAddr
   MUAMaxReTxNum        5
```

Configuring the MGCP Gateway

To configure the gateway, the following information is required:

- Authentication information required by the MGCP server (user ID).
- The supported CODECs and the order that they are proposed in negotiations.
  Up to four CODECs can be configured. The supported CODECs are G.711 u-law, G.711 a-law, and G.729 with a 10ms or 20ms RTP packet interval.
- Feature activation for RFC 2833 for DTMF, modem pass-through, or fax pass-through.
  For a modem, you can configure the port to enable modem pass-through and force media to G.711 echo cancellation (**mpt on**).
  For a fax, you can configure the port to support fax pass-through and force media to G.711 echo cancellation (**fax cc_on**).

Configuration Restraints

- Before you configure the gateway, you must configure the MGCP session controller, and the gateway settings for the MGCP protocol and the FXS port. See "MGCP Session Controller Configuration" (page 215), "Configuring MGCP Settings for the Gateway" (page 222), and "FXS Port Configuration" (page 238).
- A codec parameter that is specified as **notused** acts as a terminator in the preferred codec list; subsequent codecs are ignored.

  For example, if the codec parameters are set as below, **codec3** and **codec4** are ignored; they are not proposed in negotiations:

  ```
  codec1 PCMU_10
  codec2 notused
  codec3 PCMU_20
  codec4 PCMA_20
  ```

- Currently, Fax T.38 is not supported.
- If the FXS port is configured as a SIP gateway, that configuration must be deleted before you can reconfigure the port as an MGCP gateway.

MGCP Gateway Configuration Command

To configure the MGCP gateway, enter the following command:

```
> config mgcp ua port
```

Table 73 describes the parameters for **config mgcp ua port**.

Table 73. MGCP Gateway Configuration Parameters

Parameter	Description
[port]	Number of the FXS port (**1**).
name	Name for the display.
userid	User ID to form the MGCP Endpoint ID. This parameter is required.
codec1	Most preferred codec and packet time selection (**PCMU_10** | **PCMU_20** | **PCMA_10** | **PCMA_20** | **G729A_10** | **G729A_20** | **NOTUSED**). The default is PCMU_20.
codec2	Second preferred codec and packet time selection (**PCMU_10** | **PCMU_20** | **PCMA_10** | **PCMA_20** | **G729A_10** | **G729A_20** | **NOTUSED**). The default is PCMA_20.
codec3	Third preferred codec and packet time selection (**PCMU_10** | **PCMU_20** | **PCMA_10** | **PCMA_20** | **G729A_10** | **G729A_20** | **NOTUSED**). The default is G729A_20.
codec4	Fourth preferred codec and packet time selection (**PCMU_10** | **PCMU_20** | **PCMA_10** | **PCMA_20** | **G729A_10** | **G729A_20** | **NOTUSED**). The default is NOTUSED.

Table 73. MGCP Gateway Configuration Parameters (continued)

Parameter	Description
rfc2833	Indicates whether to use RFC 2833 for DTMF (**yes** | **no**). (RFC 2833 provides *out of band DTMF* event reports.) The default is **yes**. Distortion from compression and decompression can prevent recognition of pure DTMF tones. Out-of-band DTMF sends the information by separate RTP packets.
payload	If RFC 2833 is enabled (**rfc2833 yes**), you can specify the RTP dynamic payload type (96-127). The default is **101**.
mpt	Enables modem pass-through and forces media to G.711 echo cancellation (**on**). Specify **on** if a modem is connected to the FXS port. The default is **off**.
fax	Enables fax pass-through and forces media to G.711 echo cancellation (**off** | **cc_on**). Specify **cc_on** if a fax machine is connected to the FXS port. The default is **off**.
vad	Feature currently not supported. (Enables Voice Activity Detection (VAD) (silence suppression) (**yes** | **no**). The default is **no**. Enabling VAD allows the unit to conserve resources by avoiding sending silent RTP packets. However, VAD can silence very low sounds, lowering voice quality.)
up	Indicates whether the MGCP gateway port is enabled (**yes** | **no**). The default is **yes**.

MGCP Gateway Example

This example configures the MGCP gateway to provide VoIP connections for an analog telephone:

Name for the display: uap1
User ID: uap1
RFC2833 DTMF: yes
RFC2833 payload type: 96

```
> config mgcp ua port 1 name uap1 userid uap1 rfc2833 yes
payload 96
*> save
```

Show MGCP Gateway Configuration

To show the configuration of the MGCP gateway for port 1, enter the following command:

```
> show mgcp ua port 1

MGCP User Agent:

Port  Name        Codec1     Codec3     RFC2833 MPT  VAD
      UserID      Codec2     Codec4     Payload Fax  Up
```

```
------------------------------------------------------------
0-1   uap1        PCMU_20    G729A_20   yes     Off  no
      uap1        PCMA_20    NOTUSED    96      Off  yes
```

Delete MGCP Gateway Configuration

To delete the MGCP gateway configuration for the FXS port, enter the port number on a **del mgcp ua port** command. This allows for reconfiguration starting from default values; this is also required if the port is to be reconfigured as a SIP gateway.

NOTE: A port currently in use cannot be deleted.

For example, the following command deletes the MGCP gateway configuration for port 1:

```
> del mgcp ua port 1
```

Show MGCP Gateway Status

To show the status of the MGCP gateway, enter the following command:

```
> show mgcp ua status

MGCP UA Ports:

Port  LineStatus
------------------------------------------------------------
0-1   Inactive
```

The `LineStatus` field reports the status of the analog device:

`Inactive`	The port is not up.
`Idle`	The analog device is on-hook.
`OB (OutBound) Calling`	The analog device is off-hook or a phone number is being dialed.
`OB (OutBound) Proceeding`	The remote party is ringing.
`IB (InBound) Proceeding`	The analog device is ringing.
`Disconnecting`	The remote party is disconnected.
`Connected`	The analog device is in communication.

Show Media Stream Status

To see the current status of the VoIP media stream that terminates at the MGCP gateway, enter the following command:

```
> show media stream

Media Stream

Chan  LocalNumber     CodecType  LocalConn              RtcpTx    RtpTx
Port  RemoteNumber    CodecState RemoteConn             RtcpRx    RtpRx
------------------------------------------------------------------------
```

```
0     30008          G711u      127.0.0.1:14376          5          1491
7     30016          STARTED    127.0.0.1:14378          5          1492
```

- The **LocalConn** and **RemoteConn** fields report the IP address and RTP port for the local and remote connections.
- The **Codec Type** and **Codec State** fields report that the connection is started and using the CODEC G.711 u-law.
- The **RtcpTx** and **RtcpRx** fields report the number of RTCP packets transmitted and received.
- The **RtpTx** and **RtpRx** fields report the number of RTP packets transmitted and received.

MGCP Endpoints

This section provides guidelines to configure the MGCP endpoints that are managed by the BSGX4e device.

To enable an MGCP endpoint to place and receive calls, it must be:

- Allowed access by the Access Control List (ACL). See "Access Control List (ACL)" (page 232).
- Registered with the MGCP server through the MGCP session controller.

These requirements also apply to the MGCP gateway because the MGCP session controller handles the gateway as an MGCP endpoint. However, unlike other endpoints, an ACL entry cannot be configured to disallow the MGCP gateway. It is automatically allowed to place and receive calls and cannot be disallowed.

Preparing Endpoints for Registration

The MGCP endpoints need to be registered to the MGCP server through the MGCP session controller by using the MGCP method RSIP. To be registered, the MGCP endpoints must be configured as following:

- The MGCP endpoint identification must be per MAC address.
- The MGCP call agent must be the LAN IP address of the BSGX4e device.
- The MGCP call agent port must be the one configured as the LAN Rx port for the MGCP session controller.

For example, for a Cisco MGCP phone 7960, firmware P0M3-07-5-00, the following configuration is required (interactive menu or text configuration file):

- **use_mac_name:** 1 (enabled)
- **mgcp_gw_controller:** LAN IP address of the BSGX4e device
- **mgcp_output_port:** LAN RX port of the MGCP session controller

Verify Endpoint Registration

To verify that the endpoints are correctly registered, enter the following command:

```
> show mgcp sc endpoints


MGCP Session Controller endpoints:
Endpoint ID                EP Addr      EP Port   Act Calls
Endpoint Name              TelNo        CA Port   Timeout
-------------------------------------------------------------
4083746017@00152b177677    10.0.1.57    2427      0
Sophia 6017                6017         2432      3436
4083747001@001111111111    127.0.0.1    2429      0
                                        2429      3434
```

The entry for the MGCP gateway can be distinguished from the other endpoints because its `EP Addr` is set to the loopback IP address `127.0.0.1`.

13
VoIP Configuration

This chapter and the next chapter cover topics common to VoIP configuration for both MGCP and SIP, including:

- Media connections controlled by the **Media Bridge (MBR)**.
- Endpoint access controlled by the "Access Control List (ACL)" (page 232).
- "Cisco Discovery Protocol (CDP)" (page 234)
- Call admission based on available bandwidth as determined by the "Call Admission Control (CAC)" (page 236).
- "FXS Port Configuration" (page 238)
- Call quality analysis by "Voice Quality Monitoring (VQM)" (page 247).
- Detailed "Call Records" (page 253)
- "Local Call Routing (LCR) Mode" (page 256)

You can configure the BSGX4e device to act as both VoIP session controller and VoIP gateway. The session controller and VoIP gateway can use either the Session Initiation Protocol (SIP) or the Media Gateway Control Protocol (MGCP). Configuration for SIP is described in "SIP Configuration" (page 263). Configuration for MGCP is described in "MGCP Configuration" (page 209).

Media Bridge (MBR)

Settings for the Media Bridge (MBR) specify how VoIP media connections are established:

- By default, communication streams are established between each party and the BSGX4e. The BSGX4e bridges them to establish the end-to-end communications.
- If the direct media (**dm**) setting is enabled, communication streams are directly established between parties in a LAN-to-LAN call.

Media Settings Command

To set the parameters for VoIP media streams in the device, enter the following command:

```
> config media settings
```

Table 74 describes the parameters for **config media settings**.

Table 74. Media Stream Parameters

Parameter	Description
dm	Enables use of direct media (RTP) connections between two LAN endpoints. Initially, direct media connections are disabled.
rtp	Range of RTP ports to use (low#-high#). The RTP range must contain at least 1000 values and must not overlap ports configured for existing services in the device. Normally, two ports in the range are used for each media connection, one for RTP and the other for RTCP. The default is **13000-14999**.
audioqos	GoS quality group used to ensure voice quality. VoIP media streams are sensitive to packet delay and packet loss; if packets are dropped or delayed, voice quality deteriorates. You must configure the quality group before it can be specified as the *audioqos* value (see "GoS Configuration" (page 181)).
maxconn	Maximum number of VoIP connections (for both SIP and MGCP) allowed. The default is **500** connections.

Media Settings Example

This example configures the Media Bridge as follows:

Direct media connections between LAN endpoints: yes
RTP port range: 10000-11999
Name of GoS quality group to protect media streams: VoIPMedia

```
> config media settings dm yes rtp 10000-11999 audioqos
VoIPMedia
*> save
```

Show Media Settings

To show the current media settings, enter the following command:

```
> show media settings

Media config:
   DM Enabled     Yes
   RTP Ports      10000 - 11999
   Audioqos       VoIPMedia
   MaxConn        500
```

Show Media Status

To show the current media status, enter the following command:

```
> show media status
```

```
Media status:
  Max. cap (max_conn/AudioQos):       500/890000
  Port usage (current/highest):       0/0
  Conn usage (current/highest):       0/0
  AudioRate usage (current/highest):  0/0
```

Field	Description
Max. cap	Maximum capacity (configured maximum number of connections [*maxconn*] and the maximum available bandwidth of the quality group managing the VoIP media traffic in bits/second).
Port usage	Current number of ports in use and the highest number of ports that have been used.
Conn usage	Current number of VoIP connections and the highest number of VoIP connections.
AudioRate usage	Current and highest VoIP media rates in bits per second.

Show Media Connection Statistics

The following command displays the list of VoIP media connections established by the Media Bridge:

```
> show media connection

Media Connections:

From IP (In)  To IP (In)    From IP (Out) To IP (Out)   Mode
Port          Port          Port          Port
------------------------------------------------------------
10.0.20.2     10.0.1.1      172.29.250.5  172.29.250.30 Bridge
29268         13006         13006         29490
10.0.20.2     10.0.1.1      172.29.250.5  172.29.250.30 Bridge
29269         13007         13007         29491
```

Each call entry shows the IP addresses and ports used for the inbound connection (`In`) and for the outbound connection (`Out`).

The detailed statistics kept for each call by the session controller also list information about the outbound (`<==`) and inbound (`==>`) media connections. The following example shows SIP call statistics:

```
> show sip sc calls

SIP Session Controller detailed call entries:

EP CallInfo         Call to:  4945
   EP Info          nortel.two, 10.0.20.2:5060
   Line State       CALL_ANSWER_ACKED
   Wan ToTag        2079605163-1140867899608
   Wan FromTag      3-25-85680fc8-00005af2
```

```
Wan CallID        3-25-85680fc8-00001e5c@172.29.250.5
Lan ToTag         3-25-85680fc8-00007b76
Lan FromTag       000f8f07308800076d578d1c-7d53b8e2
Lan CallID        000f8f07-30880004-51dee830-20cc6f3b@10.0.20.2
Media Mode        NORMAL
Media Type        AUDIO
Media Conn_b       172.29.250.30:29490--172.29.250.5:13006<==
Media Conn_a             ==>10.0.1.1:13006--10.0.20.2:29268
```

- Media Conn_b shows the IP addresses and ports used for the outbound connection.
- Media Conn_a shows the IP addresses and ports used for the inbound connection.

The following command displays detailed information about MGCP calls:

```
> show mgcp sc calls

MGCP Session Controller detailed call entries:

EP Call Info          Call to:  6019
   EP Info            4083747001@001122334455, 127.0.0.1:0
   Line Number        1
   Line State         CALL_CONNECTED
   Media Conn Mode    NORMAL
   Media Type         AUDIO
   Media Conn_b        66.206.164.199:32046--66.206.164.203:13024<==
   Media Conn_a             ==>127.0.0.1:13024--127.0.0.1:32100
```

Access Control List (ACL)

The Access Control List (ACL) is a list of policy entries that determine which LAN endpoints are allowed to place and receive calls. By default, the ACL includes a policy that allows all LAN endpoints to place and receive calls. To deny an endpoint call access, you must add a policy denying access to the ACL.

When an endpoint attempts to place or receive a call, authentication is performed. Information about the endpoint is compared to the policy entries in the ACL to determine if the endpoint is given access. Information about the endpoint is provided by the session controller and, if available, by the Cisco Discovery Protocol (CDP).

The session controller provides the following information:

- MAC address
- IP address
- Signaling type
- Endpoint ID

CDP can provide this information:

- Device ID

- Platform
- Software version

NOTE: The ACL does not require CDP information; the use of information provided by CDP is optional. For more information about CDP, see "Cisco Discovery Protocol (CDP)" (page 234).

Access Control List Command

To create an entry in the Access Control List (ACL), enter the following command:

```
> config voice acl
```

Table 75 describes the parameters for **config voice acl**. Omitted authentication parameters are set to **any**, indicating that all values match.

Table 75. Voice ACL Parameters

Parameter	Description
[id]	Unique numeric identifier of the policy. Specify **new** to create a new policy.
mac	MAC address of the endpoint.
epid	ID of the endpoint.
softversion	Software version of the endpoint.
platform	Platform type of the endpoint.
deviceid	Device ID of the endpoint.
seq	Sequence number of the policy (**begin** | **end** | **position**).
ip	Single IP address or a range of addresses for the endpoints.
type	Signaling type of the endpoint (**any** | **mgcp** | **sip**). The default is **any**.
action	Indicates the access given by this entry (**deny** | **allow**). The default is **allow**.

ACL Entry Example

This example configures a new ACL policy. The entry denies access to the LAN endpoint with the specified IP address, signaling type, and device ID, as follows:

IP address: `10.0.1.100`
Signaling type: `SIP`
Device ID: `SIP000F8F073088`
Action: `deny`

```
> config voice acl new ip 10.0.1.100 type sip deviceid
SIP000F8F073088 action deny
*> save
```

This example configures an ACL entry for an MGCP endpoint, as follows:

IP address: 10.0.1.100
Signaling type: MGCP
Device ID: MGC000F8F073088
Action: deny

```
> config voice acl new ip 10.0.1.100 type mgcp deviceid
MGC000F8F073088 action deny
*> save
```

Show ACL

To list the current ACL policies, enter the following command:

```
> show voice acl

Session Controller - ACL:

Id Seq EpId     Platform  IP             MAC Address     Action
       Software DeviceId                 Type            Stats
-------------------------------------------------------------------
1  1   any       any      10.0.1.100     any             deny
       any       SIP000F*                sip             0
```

- The asterisk at the end of the device ID (SIP000F*) indicates that only the first part of the device ID is shown.
- The **Stats** field reports the number of times an endpoint is matched to this policy.

Cisco Discovery Protocol (CDP)

The BSGX4e device supports Cisco Discovery Protocol (CDP) versions 1 and 2 to report the presence of CDP-capable neighbors, such as Cisco VoIP phones. CDP discovers devices both on the LAN and on the WAN.

The BSGX4e device analyzes CDP packets received from the network. It does not transmit CDP packets to provide information about the system to its neighbors.

Information that CDP retrieves about LAN devices can be used to check their configurations. The information is also used by the Access Control List (ACL). See "Access Control List (ACL)" (page 232).

NOTE: CDP is always running. It cannot be disabled.

Show CDP Entry

To see the information CDP about the current neighbors, enter the following command:

```
> show cdp entry
```

```
CDP Entry:

Device ID:          SIP00152B1775ED
Entry Address:      192.168.1.10
Prefix:             0.0.0.0
Platform:           Cisco IP Phone 7960
Interface:          Port 1
HoldTme:            121
Version:            P0S3-07-5-00
Duplex:             Full
Power:              6300

CDP Entry:
Device ID:          MGC0009E8812FDB
Entry Address:      66.206.164.221
Prefix:             0.0.0.0
Platform:           Cisco IP Phone 7960
Interface:          Port 1
HoldTme:            135
Version:            P0M3-07-3-00
Duplex:             Half
Power:              6300
```

Show CDP Neighbors

To see a summary of the current neighbors, enter the following command:

```
> show cdp neighbors

CDP Neighbors:
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID       Intf Hold Capability Platform               Port
ID
-------------------------------------------------------------------
SIP000F8F072D3D eth1 130  H          Cisco IP Phone 7960      Port 1
CCM.acme.com    eth0 129  H         Win2000 Server           Eth 1/1
SEP0004f2034175 eth0 156  H          Polycom SoundPoint IP    Port 1
SIP000F8F072DB5 eth0 159  H          Cisco IP Phone 7960      Port 1
SIP000F8F072DB5 eth0 159  H          Cisco IP Phone 7960      Port 1
c2520           eth0 129  R         cisco 2520               Ethern*
```

- The `Intf` field reports the device location (`eth1` indicates the device is on LAN; `eth0` indicates the device is on the WAN).
- The `Hold` field reports the time to live (TTL) value for the device.
- The `Capability` field reports the role of the device:
  - R: router
  - T: transparent bridge
  - B: source route bridge

- S: switch
- H: host
- I: IGMP capable device

Show CDP Statistics

To view the statistics for the CDP protocol, enter the following command:

```
> show cdp traffic

CDP traffic:

Total CDP packets in:     2021
CDP checksum errors:      0
CDP Ver1 packets in:      0
CDP Ver2 packets in:      2021
```

Call Admission Control (CAC)

When the session controller receives a request to place or receive a call, Call Admission Control (CAC) determines if the call can be allowed within the configured limits.

NOTE: By default, the SIP session controller does not apply CAC to local or PSTN calls. A session controller setting can enable CAC for calls between LAN endpoints.

CAC rejects the call if its admission would exceed any of the following limits:

- **Maximum number of calls** allowed by the session controller (SIP or MGCP **maxcalls** parameter; default, **500**).
- **Maximum number of VoIP media streams** allowed (**maxconn** parameter, default **500**).
- **Maximum bandwidth** allowed by the appropriate GoS quality group (no defaults)**.** Two quality groups protect VoIP traffic: one protects signaling traffic (**sigqos** parameter) and the other protects media traffic (**audioqos** parameter).

The **maxcalls** and **sigqos** parameters are specified on the session controller setting command (see “Session Controller Setting Command” (page 272) or “Session Controller Setting Command” (page 216)). The **maxconn** and **audioqos** parameters are specified on the **config media settings** command (see “Media Settings Command” (page 229)).

VoIP Bandwidth Requirements

Bandwidth allocation is required for VoIP signaling traffic and for VoIP media streams. You can assign separate GoS quality treatment to each traffic type. The quality treatment is defined by the quality groups specified by the **sigqos** and **audioqos** parameters. For more information about GoS bandwidth allocation and quality protection, see “GoS Configuration” (page 181).

The bandwidth allocated for VoIP signaling traffic can administratively limit the number of calls. It is typically defined by the ISP based on the number of users.

The bandwidth allocation for VoIP media streams should accommodate the expected call load. If bandwidth is to be available for the maximum number of calls regardless of the level of other traffic on the network, then the **audioqos** quality group must commit sufficient bandwidth for the maximum connections (**maxconn**).

Calls are rejected if WAN bandwidth is unavailable. This is necessary because call admission without sufficient bandwidth results in VoIP packets being dropped, and thus, poor voice quality.

The maximum connections (**maxconn**) limit does not distinguish between VoIP media streams of different CODECs (and so of different rates). However, the CODECs in use do affect the bandwidth required and so affect the number of calls that can be carried by a given bandwidth. Based on CODEC negotiation, the session controller deduces how much bandwidth is required to establish the call. It then checks if that bandwidth is available within the quality group allocation, and finally, decides to accept or reject the call.

NOTE: It is strongly recommended that every VoIP quality group be assigned to GoS class A1. This guarantees the least possible delay and the lowest percentage of packets dropped. It is also strongly recommended that the quality group use the strict policing method. This method guarantees a fixed maximum output rate, regardless of other traffic on the network.

Show Call Admission Settings

To see the current settings for the VoIP media quality group (Audioqos) and maximum connections (MaxConn), enter the following command:

```
> show media settings

Media config:
   Direct Media Enabled   No
   RTP Ports      13000 - 14999
   Audioqos       VoIPMedia
   MaxConn        500
```

To see the current session controller setting for the maximum allowed calls (CAC maxcalls), enter one of the following commands:

```
> show sip sc status

SIP Session Controller status:
   SSC Started          Yes
   SSC Server Ready     Yes
   My Wan IpAddr        172.29.250.5
   Wan Rx Port          5060
   Lan Rx Port          5060
   CAC Max Calls        500
```

```
> show mgcp sc status

MGCP Session Controller status:
   MSC Started          Yes
   MSC Server Ready     Yes
   My Wan IpAddr        192.168.134.217
   Wan Rx Port          2427
   Lan Rx Port          2427
   CAC Max Calls        500
```

The field CAC Max Calls reports the maximum number of calls allowed.

To see the current VoIP connection and call status, enter the following command:

```
> show media status

Media status:
  Max. cap (max_conn/qos_bps):      500/1000000
  Port usage (current/highest):     0/0
  Conn usage (current/highest):     0/0
  Rate usage (current/highest):     0/0
```

The line labeled Max. cap (max_conn/qos_bps) reports both the configured maximum number of connections (max_conn) and the maximum available bandwidth of the quality group managing the VoIP media traffic in bits per second.

FXS Port Configuration

You can configure the following settings for the FXS port:

- The unit name (identifies the BSGX4e device).
- A country code that automatically adjusts the parameter settings of the port to the specific values required by the selected country.

If the device is to be configured for a country whose country code is not currently supported, explicit configuration of the following features can be required:

- Jitter buffer settings.
- DSP gain values.
- Call progress tones.
- Impedance override settings.

The FXS port can also be tested using line fault testing (the GR-909 metallic loop tests).

CAUTION: Except for the unit name and country code, do not change FXS port settings without expert assistance.

Country Code and Unit Name Setting

Countries have defined separate telephony standards, including interface requirements, tone definitions, and ringing cadences. You can load the appropriate parameters in to the unit by configuring the country code; only the country code needs to be configured.

NOTE: The unit must be restarted for a country code change to take effect.

The default unit name is *MyUnit*. You can change it to any meaningful identifier.

To configure the country code for the FXS port, enter the following command:

```
> config system info
```

Table 76 describes the parameters for **config system info**.

Table 76. System Info Parameters

Parameter	Description
unit	Unit name of the device. Specify this parameter only if the name is to be changed.
country	Two-letter country code as defined by ISO-3166. Currently, the only country codes supported are for the United States (**US**), Canada **(CA)**, China (**CN**), and New Zealand (**NZ**).

Country Code Setting Example

The following example changes the country code to CN for China:

```
> config system info country CN
*> save
> reload
```

Show Country Code

To show the country code of the FXS port, enter the following command:

```
> show system info
System Info:

   Unit Name       MyUnit
   Bootcode Ver    1.10.0009
   App. Ver        BSG T2
   System Type     BSGX4e
   Memory          89/128 MB
   MAC 0           00:22:11:44:33:04
   MAC 1           00:22:11:44:33:05
   Serial
   Country         China (CN)
   Temp            Unsupported
   Up time         0y 0d 4h 33m 20s
```

The display shows the country code as CN for China.

Jitter Buffer Settings

To configure the jitter buffer for the FXS port, enter the following command:

```
> config voice jitterbuffer
```

Table 77 describes the parameters for **config voice jitterbuffer**.

Table 77. Voice Jitter Buffer Configuration Parameters

Parameter	Description
mode	Jitter buffer type (**fixed** | **adaptive**).
maximum	Maximum delay introduced by the jitter buffer (ms). This value is used only if **mode** is **adaptive**. The default value is **120** ms.
nominal	Nominal delay introduced by the jitter buffer (ms). The default value is **40** ms.
minimum	Minimum delay introduced by the jitter buffer (ms). This value is used only if **mode** is **adaptive**. The default value is **20** ms.

Jitter Buffer Example

This example configures the FXS port as follows:

Country: US
Jitter buffer: Fixed mode
Nominal delay: 60 ms

```
> config system info country US
*> config voice jitterbuffer mode fixed nominal 60
*> save
```

Show Jitter Buffer Settings

To show the jitter buffer configuration of the FXS port, enter the following command:

```
> show voice jitterbuffer
Voice Jitter Buffer Settings:

   Mode        fixed
   Maximum     120 ms
   Nominal     60 ms
   Minimum     20 ms
```

Show Jitter Buffer Statistics

To see the jitter buffer statistics, enter the following command:

```
> stats voice jitterbuffer
```

```
Jitter Buffer Stats:

Port RxFrames      CurrJitter    CurrDelay     MinDelay    MaxDelay
     Overflowed    Underrun      OutOfOrder    Duplicated  LateDropped
-------------------------------------------------------------------------
1    1786          2             20            20          21
     0             0             0             0           0
```

The following are descriptions of the jitter buffer statistics:

Statistic	Description
RxFrames	Number of packets received.
CurrJitter	Current average jitter detected.
CurrDelay	Current packet delay due to the jitter buffer (in milliseconds).
MinDelay	Minimum packet delay due to the jitter buffer (in milliseconds).
MaxDelay	Maximum packet delay due to the jitter buffer (in milliseconds).
OverFlowed	Number of packets dropped due to overflow.
UnderRun	Number of packets dropped due to underrun.
OutOfOrder	Number of packets out of order.
Duplicated	Number of packets dropped due to duplication.
LateDropped	Number of packets dropped due to late arrival.

Call Progress Tones

To configure DSP call progress tones, each tone type is assigned its correct cadence, frequency, and level values. You can configure the following tone types:

dial tone	**call waiting tone 1**
ringback tone	**call waiting tone 2**
busy tone	**reorder tone**
congestion tone	**stutter dial tone**
test tone	**off hook warning tone***

NOTE: Configuration of the off hook warning tone can require a third cadence and frequency/level pair. The parameters for those values are not currently supported.

Show Call Progress Tones

To show the current configuration of the call progress tones for the FXS port, enter the following command:

```
> show voice tones

DSP Tone Settings
```

```
Tone Type    On-1 Off-1 On-2 Off-2 Freq1 Level1 Freq2 Level2
-------------------------------------------------------------
none         0    0     0    0     0     0      0     0
dial         500  0     0    0     350   -24    440   -24
ringback     2000 4000  0    0     440   -24    480   -24
busy         500  500   0    0     480   -24    620   -24
congestion   250  250   0    0     480   -24    620   -24
callwait1    300  300   0    0     440   -24    250   -24
callwait2    300  300   0    0     440   -24    250   -24
reorder      250  250   0    0     480   -24    620   -24
stutter      100  100   0    0     350   -24    440   -24
offhookwarn  250  250   0    0     1430  -24    2500  -24
test         4000 0     0    0     1000  -24    1000  -24
```

Re-configure Tones

To configure a tone type for the FXS port, enter the following command:

```
> config voice tones
```

Table 78 describes the parameters for **config voice tones**.

Table 78. Call Progress Tone Parameters

Parameter	Description
[tone]	Tone type to be reconfigured by the command (**dial** | **ringback** | **busy** | **congestion** | **callwait1** | **callwait2** | **reorder** | **stutter** | **offhookwarn**| **test**). This parameter is required.
on1 **off1**	Use these two parameters to redefine the first ringing cadence.
on2 **off2**	Use these two parameters to redefine the second ringing cadence.
freq1 **level1**	Use these two parameters to redefine the first frequency/level pair.
freq2 **level2**	Use these two parameters to redefine the second frequency/level pair.

Configuration Example

The following commands redefine values for the call progress tones:

```
> config voice tones dial on1 500 off1 0 on2 0 off2 0 freq1
425 level1 -10 freq2 0 level2 0
*> config voice tones ringback on1 1000 off1 4000 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0
*> config voice tones busy on1 330 off1 330 on2 0 off2 0 freq1
425 level1 -10 freq2 0 level2 0
```

```
*> config voice tones congestion on1 150 off1 150 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0
*> config voice tones callwait1 on1 200 off1 5000 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0
*> config voice tones callwait2 on1 100 off1 1000 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0
*> config voice tones reorder on1 250 off1 250 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0
*> config voice tones stutter on1 400 off1 40 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0
*> config voice tones test on1 500 off1 0 on2 0 off2 0 freq1
1000 level1 -10 freq2 0 level2 0
*> save
```

DSP Gain Settings

To set the DSP gain values for the FXS port, enter the following command:

```
> config voice fxs gain
```

This commands parameters are as follows:

Parameter	Description
tx	Transmit (tx) gain (digital to analog conversion) in decibels. Specify a minus (-) before a negative value. The default is **-3** dB.
rx	Receive (rx) gain (analog to digital conversion) in decibels. Specify a minus (-) before a negative value. The default is **-3** dB.

Show Gain Settings

To show the DSP gain settings, enter the following command:

```
> show voice fxs gain

FXS Gain Global Settings:

   Tx      -3 dB
   Rx      -3 dB
```

Line Impedance Settings

To set a line impedance value for the FXS port, enter the following command:

```
> config voice fxs hw
```

This commands parameter is as follows:

Parameter	Description
impedance	Specialized impedance override setting for the line (automatic | 600 | 900 | 600_luF | 900_2.16uF | 270+750_150nF | 220+820_120nF | 220+820_115nF | 200+680_100nF). The default is **automatic**.

Show Impedance Settings

To show the impedance setting, enter the following command:

```
> show voice fxs hw

FXS Global HW Settings:

   Impedance     Automatic
```

Electrical Status

To show the current electrical values for the FxS port, enter the following command:

```
> show voice fxs status

FXS Status:

Port Line State Battery (V) Line (V) Current (mA) Power (mW)
-------------------------------------------------------------
0-1  Ready      61          49       0            0
```

Field	Description
Port	Unit and port number.
Line State	The possible line states are: Open-Cct Open Circuit. Ready Fwd-OHT Forward On-hook Transmission. Tip-Open Ringing Rev-actionReverse Active. Rev-OHT Reverse On-hook Transmission. Ring-Open Thermal Failed
Battery	Scaled battery voltage measurement in the range 0-327 Volts.

Field	Description
Line	Loop voltage measured across TIP-RING in the range 0-327 V. While the phone is on-hook, the value is expected to be in the range 4-18 V. A value outside this range can indicate a problem. If the phone is not connected, the value is undetermined.
Current	Current in milliamps.
Power	Power in milliwatts.

Line Fault Testing

You can test the electrical status of the FXS port using the GR-909 metallic loop tests.

NOTE: The GR-909 tests are for diagnostic purposes only. Do not run the tests on a port that is in use. Running a test on a busy port aborts the call on that port.

Voltage Tests

The GR-909 voltage tests are as follows:

- **Hazardous voltages**
  This test fails if an AC voltage greater than 50 Volts Root Mean Square (Vrms) or a DC voltage greater than 135 Volts Direct Current (VDC) is measured on the tip pin or ring pin.
- **Foreign voltages test**
  This test fails if a tip pin or ring pin AC voltage is greater than 10 Vrms or if a tip pin or ring pin DC voltage is greater than 6 VDC. This test is performed when it is determined that a hazardous voltage is not present on the line.

To initiate the hazardous voltages test and display its results, enter the following command:

```
> show voice fxs gr909 voltages
```

To initiate the foreign voltages test and display its results, enter the following command:

```
> show voice fxs gr909 foreignvoltages
```

For example, the following command runs the foreign voltages test for FXS port 1:

```
> show voice fxs gr909 foreignvoltages
```

```
FXS GR909 foreign voltages (* is a failure)
Port dcVtip  dcVring  dcVloop
     acVtip  acVring  acVloop
-------------------------------------------------------------
1     3      52       -48
      0      0        0
```

If a test fails, an asterisk is shown.

Resistance Tests

The GR-909 resistance tests are as follows:

- **Resistive faults test**
  This test fails if a Tip/Ring, Tip/Ground, or Ring/Ground on-hook DC resistance less than 150k ohms is measured.
- **Receiver off-hook test**
  This test is used to discriminate between a resistive fault and an off-hook condition. It uses a procedure similar to the resistive faults test, but it is measured across Tip/Ring only. Also, two measurements are performed at different open circuit voltages to verify the resistive linearity. If the calculated resistance shows less than 15% nonlinearity between the two calculated points and the voltage/current origin, it is determined to be a resistive fault.

Resistive Faults Test

To initiate the resistive faults test and display its results, enter the following command:

```
> show voice fxs gr909 resistances
```

For example, the following command tests the resistances for FXS port 1:

```
> show voice fxs gr909 resistance

FXS GR909 resistances (* is a failure)
Port RTG   RTR     RRG
-------------------------------------------------------------
1    OK    <<150K  OK
```

If a test fails, an asterisk is shown. The tests are labeled as:

- RTG: Resistor Tip to Ground
- RTR: Resistor Tip to Ring
- RRG: Resistor Ring to Ground

The value for each test is either <<150K, indicating a measurement less than 150K ohms or OK, indicating a measurement greater than 150K ohms.

Receiver Off-Hook Test

To initiate the receiver off-hook test and display its results, enter the following command:

```
> show voice fxs gr909 offhook
```

For example, the following command runs the off-hook test for FXS port 1:

```
> show voice fxs gr909 offhook

FXS GR909 off hook (* is a failure)
Port Off-hook
-------------------------------------------------------------
1    no
```

REN Test

The GR-909 ringing equivalency number (REN) value expresses the total loading effect of the equipment on the ringing current generator. The REN test verifies the presence of equipment (including, phone, fax, modem) at the end of the TIP/RING pair. The REN for most modern telephones is usually less than 1.

The REN test fails if it measures less than 0.175 REN (less than 40k ohms) or greater than 5.0 REN (greater than 1400 ohms). A returned value of less than 1400 ohms is determined to be a resistive fault from TIP-RING, and a returned value of greater than 40k ohms is determined to be a loop with no handset attached.

To initiate the REN test and display its results, enter the following command:

```
> show voice fxs gr909 ren
```

For example, the following command tests the REN for FXS port 1:

```
> show voice fxs gr909 ren

FXS GR909 REN (* is a failure)
Port REN
-------------------------------------------------------------
1    .175<REN<1
```

The example above shows a success. If the REN test fails, either `*REN<.175` or `*REN>5` is shown.

Voice Quality Monitoring (VQM)

To analyze and monitor voice quality, configure the Voice Quality Monitoring (VQM) analyser to do the following:

1. **Measure call quality.**

   Specify how to measure call quality. The VQM analyser simulates a jitter buffer to analyze VoIP media streams so as to deduce information such as packet loss, delay, and jitter. Based on these parameters, it calculates R-Factors/Mean Opinion Scores updated in real-time over the duration of calls.

2. **Trigger alarms.**

   Specify if alarms are to be triggered by:

   - Low quality R-factor

- Excessive bursting R-factor (low quality R-factor lasting a certain period of time)
- Excessive delay.

The alarm levels and the duration of an alarm are also specified.

Alarms are reported in the system log as INFORM messages. For more information about the system log, see "Show System Operation Summary" (page 323).

Monitored Calls

The VQM analyser reports statistics for every VoIP media stream that flows through the routing engine. The flows that are analysed depend on:

- Whether the call is a local call or an external call.
- Whether direct media (the **dm** media setting) is enabled (see "Media Settings Command" (page 229)).

For *external* calls (either from the LAN to the WAN or from the User Agent to the WAN), only the *inbound* flow (from the WAN) can be monitored by VQM.

Similarly, for *local calls between the User Agent and the LAN*, only the *inbound* flow (from the LAN) can be monitored.

However, for *local calls between LAN endpoints*, the **dm** setting determines if the flow is monitored:

- If **dm** is enabled, the session controller can directly establish RTP flows between two LAN endpoints. The VQM analyser *cannot* measure those direct media flows.
- If **dm** is disabled, the RTP flows between LAN endpoints are bridged by the routing engine and *both flows* can be measured by VQM.

Figure 15 illustrates the calls that VQM measures.

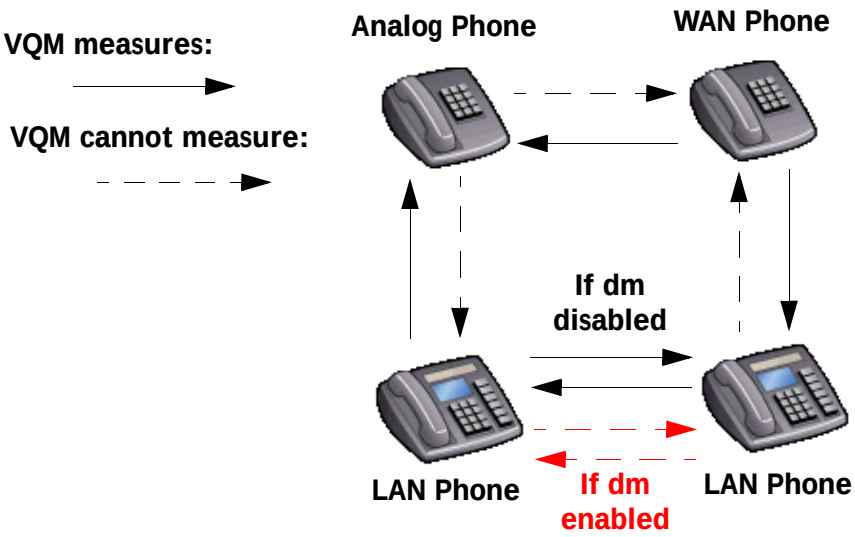


Figure 15. Flows that VQM Measures

The VQM analyser reports statistics for the following CODECs:

- G.711 u-law
- G.711 A-law
- G.726-32k
- G.728-class
- G.729-class (but not G.729D and G.729E)
- GSM Full-Rate (6.10)

VQM Analyser Command

To configure the VQM analyser, enter the following command:

```
> config calls analyser
```

Table 79 describes the parameters for **config calls analyser**.

Table 79. Call Analyser Configuration Parameters

Parameter	Description
jb	Indicates whether to emulate a static or adaptive jitter buffer (**static** | **adaptive**).
min	Minimum size of the simulated jitter buffer. The default is **10**.
max	Maximum size of the simulated jitter buffer. The default is **60**.
nom	Nominal level of the simulated jitter buffer. The default is **30**.
rtdelay	Estimate of round trip delay if no RTCP records are detected (in milliseconds). The default is **60** milliseconds.
quality	Enable alarms for low quality R-factor. The default is **yes**.
burst	Enable alarms for excessive bursting. The default is **yes**.
delay	Enable alarms for excessive delay. The default is **yes**.
rquality	Alarm trigger for low quality R-Factor. The default is **60**.
rburst	Alarm trigger for excessive bursting. The default is **60**.
burstmin	Minimum alarm trigger for excessive bursting duration (in milliseconds). The default is **500** milliseconds.
delaymax	Maximum alarm trigger for excessive delay (in milliseconds). The default is **450** milliseconds.
qalertclear	Minimum duration until the low quality alarm is cleared. The default is **3** seconds.
balertclear	Minimum duration until the excessive bursting alarm is cleared. The default is **3** seconds.
dalertclear	Minimum duration until the excessive delay alarm is cleared. The default is **3** seconds.

VQM Analyser Example

This example configures the VQM analyser as follows:

Jitter Buffer type: `static`
Alarm for low quality R-factor: `yes`
Alarm for excessive bursting R-factor: `yes`
Alarm for excessive delay: `yes`
Low R-Factor trigger: `50`
Excessive bursting R-factor trigger: `50`
Excessive bursting R-factor duration: `1000 ms`
Excessive delay: `100 ms`

```
> config call analyser jb static quality yes burst yes delay
yes rquality 50 rburst 50 minburst 1000 maxdelay 100
*> save
```

Show VQM Analyser Configuration

To show the VQM analyser configuration, enter the following command:

```
> show call analyser

Call Analyser:

   JB Type                    static
   JB Minimum                 10
   JB Maximum                 60
   JB Nominal                 30
   Roundtrip Delay            60 ms

Alarms:

   Quality                    yes
   Burst                      yes
   Delay                      yes
   R-Quality                  50
   R-Burst                    50
   Min Burst                  1000 ms
   Max Delay                  100 ms
   Min Quality Alert Clear    3 sec
   Min Burst Alert Clear      3 sec
   Min Delay Alert Clear      3 sec
```

Show VQM Call Summary

To show a summary view of the quality of voice calls, enter the following command:

```
> show call quality

Monitored Calls:

EP-ID      EP-Name    MOS-LQ MOS-CQ R Factor RTP Rx     Loss       Codec
```

```
-------------------------------------------------------------------
nortel.two   4982       4.20   4.18   92       515        0.00       PCMU
```

Field	Description
EP-ID, EP-Name	Source of the VoIP media stream monitored (its endpoint ID and endpoint name).
MOS-LQ, MOS-CQ, R Factor	Scores for Mean Opinion Score - Listening Quality, Mean Opinion Score - Conversation Quality, and R-Factor. These values depend on the CODEC used and the level of traffic disruption (for example, packet loss, delay, or jitter)
RTP Rx	Number of RTP packets received from the source.
Loss	Number of packets lost.
Codec	CODEC used by the source. (If the CODEC used is not supported by the VQM analyser, it is not listed.)

Voice Quality Statistics

The VQM statistics display shows a full view of the quality of voice calls. It displays the values of the different parameters used to estimate the quality of calls (MOS and R-Factor scores).

To show a full view of the quality of voice calls, enter the following command:

```
> stats call quality

Monitored Calls:

EP-ID   MOS-LQ RTP Rx     JB Admit   JB Early   JB OOO     JB URun
EP-Name MOS-CQ Lost       JB Disc    JB Late    JB Dup     JB ORun
-------------------------------------------------------------------
nortel.tw*4.20   884        884        1          0          0
4982    4.18   0          0          0          0          0
```

Field	Description
EP-ID, EP-Name	Source of the VoIP media stream monitored (its endpoint ID and endpoint name).
MOS-LQ, MOS-CQ	Scores for Mean Opinion Score - Listening Quality and Mean Opinion Score - Conversation Quality. These values depend on the CODEC used and on the level of traffic disruption (for example, packet loss, delay, or jitter)
RTP Rx	Number of RTP packets received from the source.
Lost	Number of packets lost.

Field	Description
JB statistics	Statistics of the simulated jitter buffer used to deduce how much VoIP traffic is disrupted. (The JB fields do not report information if the CODEC used is not supported by the VQM analyser.)

Alarm Log Entries

When a triggering threshold is reached, an alarm entry is sent to the system log. For more information about system logging, see "Show System Operation Summary" (page 323).

To see the system log entries, enter the following command:

```
> show logging internal
```

The following system log entries indicate that an alarm is detected and cleared:

```
Message
--------------------------------------------------------------------------
09:33:19: (:100001) Excessive Bursting alert on call detected
09:33:19: (:100001) Excessive Bursting alert on call cleared
```

The following information fields are included in each message:

- The first column is the time.
- The second column shows the source of the VoIP stream for which the alarm is triggered.
- The third column reports which alarm is detected or cleared:
  - `Low Quality`: low R-Factor
  - `Excessive Bursting`: excessive bursting R-factor
  - `Excessive Delay`: excessive delay

Alarm Statistics

To see the number of alarms triggered, enter the following command:

```
> show call alarms

Alarm Stats:

   Low Quality         6
   Excessive Burst     15
   Excessive Delay     0
```

The alarm statistics are:

- `Low Quality` Number of alarms reported due to a low R-Factor.
- `Excessive Burst` Number of alarms reported due to an excessive bursting R-factor.
- `Excessive Delay` Number of alarms reported due to an excessive delay.

Call Records

This section describes commands to list the calls in progress and the call history. These commands are independent of the signaling protocol used to establish calls (SIP or MGCP).

Show Current Calls

To show the current calls, enter the following command:

```
> show calls current
```

The following call list example shows two SIP calls:

```
Call List:

A Party     B Party     Type      Protocol        Start Time
A Number    B Number    State     Quality         Duration
-------------------------------------------------------------------
4982                   Outbound   SIP            FEB 25 12:49:29 2006
nortel.two    4945       Connected  4.20/4.18       73350 seconds
nortel.four             Outbound   SIP            FEB 25 12:49:58 2006
nortel.four   4983       Connected  4.20/4.18       73321 seconds
```

The following call list example shows one MGCP call:

```
Call List:

A Party     B Party      Type       Protocol     Start Time
A Number    B Number     State      Quality      Duration
-------------------------------------------------------------------
Sophia 6030 6033,Sophia  Outbound    MGCP         AUG 21 16:17:58 2006
6030        6033         Connected   4.20/4.18    39 seconds
```

Table 80 describes the call record fields.

Table 80. Call Record Fields

Field	Description
A Party	Identifier for one end of the call.
A Number	Number for `A Party` (if known).
B Party	Identifier for the other end of the call.
B Number	Number for `B Party` (if known).
Type	Reports if the call originated from the LAN (`OutBound`) or from the WAN (`InBound`).
State	Reports the current state of the call: `Proceeding`: the call is in progress. `Connected`: the call is established. `Failed`: the call terminated abnormally. `Succeed`: the call terminated normally.

Table 80. Call Record Fields (continued)

Field	Description
Protocol	Protocol that the calling party is using.
Quality	Quality of the stream coming from the WAN. It reports a RTCP-XR derived MOS quality score (MOS-LQ/MOS-CQ). If the field reports **Not measured**, either the CODEC used is not supported by VQM or RTP traffic is not received. For more information about VQM, see "Voice Quality Monitoring (VQM)" (page 247).
StartTime	Start time of the call.
Duration	Time elapsed since the start of the call.

Show Call History

A call history is kept; it can show the last 250 calls. Filled in First In First Out (FIFO) order, the latest call is inserted at the end of the list.

To show the call history, enter the following command:

```
  > show calls history
Call History:

A Party     B Party      Type         Protocol    Start Time
A Number    B Number     State        Quality      Duration
-------------------------------------------------------------------
Sophia 6030 6033,Sophia  Outbound    MGCP          AUG 21 16:17:58 2006
6030        6033         Succeeded   4.20/4.18     204 seconds
```

The call history fields are the same as the fields in the current calls display, as listed in Table 80.

14
LOCAL CALL ROUTING

This chapter describes the telephone service that the BSGX4e device can provide without the use of a VoIP call server on the WAN. This service is called local call routing or LCR mode and is available even during a VoIP service interruption.

VoIP Service Interruption

The BSGX4e device can provide backup phone service even when VoIP phone service is unavailable. As long as power is available, local call routing can connect internal calls and place external calls through the FxO port (see Figure 16).

A VoIP service interruption can occur if the WAN connection fails, the call server connection fails, or a call server is not available. However, it is not considered a service interruption when a VoIP call cannot be placed due to lack of bandwidth.

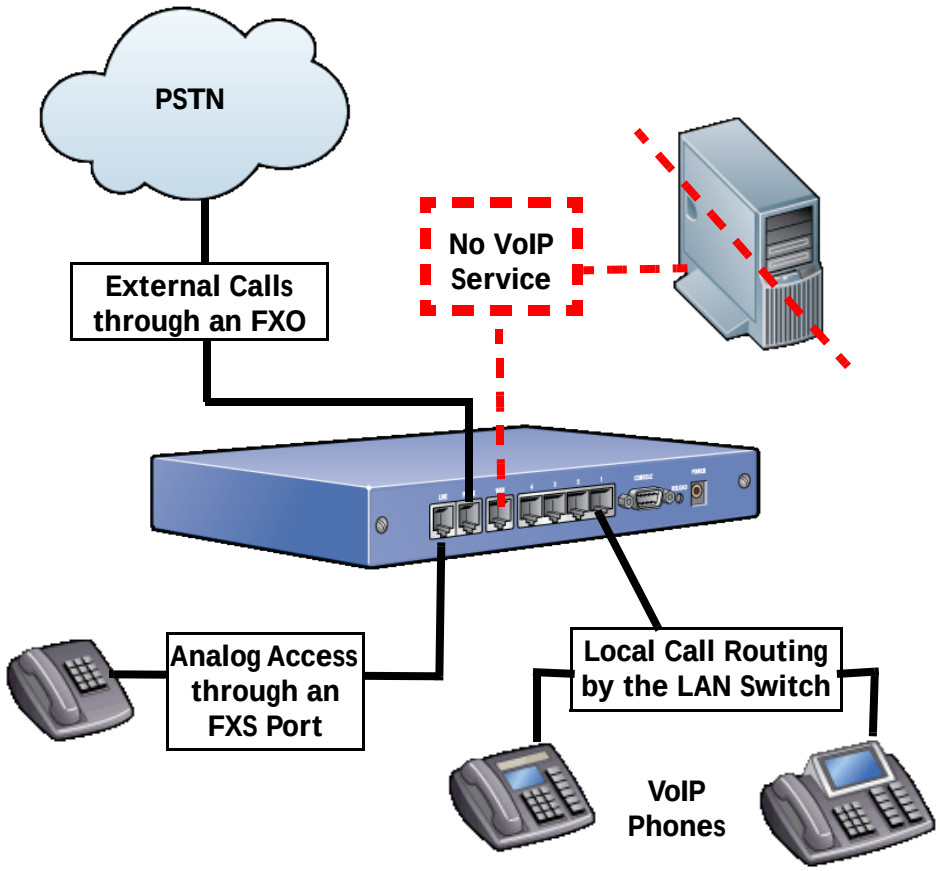

PSTN
External Calls through an FXO
No VoIP Service
Analog Access through an FXS Port
Local Call Routing by the LAN Switch
VoIP Phones

Figure 16. VoIP Service Interruption

Local Call Routing (LCR) Mode

Local call routing (LCR) mode describes the telephone service that the BSGX4e device can provide without the use of a VoIP call server on the WAN. Local call routing is automatically used when VoIP service is interrupted and LAN endpoints cannot receive or place calls using a call server on the WAN.

In LCR mode, LAN VoIP phones (and an analog device on the FXS port) can place and receive *local calls*—calls that do not go out to the WAN. Limited external call service is also available through the FXO port of the BSGX4e. If the FXO port is connected to a CO telephone line, the BSGX4e can send external calls out on the PSTN. In LCR mode, only basic telephone services are supported:

- Local calls (between LAN endpoints) are established through the BSGX4e device (acting as a VoIP server).
- Calls identified as external calls are routed to the PSTN through the FXO interface of the BSGX4e or through a SIP/PSTN gateway located in the LAN.

When VoIP call service resumes, external calls are automatically received and placed as normal.

LCR Configuration

NOTE: You must configure a VoIP session controller (SIP or MGCP) before you configure local call routing. See "SIP Session Controller" (page 264) or "MGCP Session Controller Configuration" (page 215).

LCR configuration can require:

- LCR accounts (only if LAN endpoint IDs are alphanumeric)
- LCR settings
- Telephony settings (gain and impedance for the FxO port)

LCR Account Configuration

When the BSGX4e device acts as the VoIP server to perform local call routing, it needs to know the telephone numbers of the local endpoints. An LCR account informs the BSGX4e device of the telephone number of a local endpoint when the user ID or endpoint ID does not provide that information. For example, when a SIP account is defined by a name string, the LCR account defines the telephone number of that account.

NOTE: LCR accounts are not required if the IDs of the LAN endpoints are numeric, not alphanumeric.

If LCR accounts are not configured, VoIP phones with alphanumeric IDs can only receive calls from other VoIP phones that allow the entry of alphanumeric IDs. Other entities are not able to place calls to VoIP phones that have alphanumeric IDs.

LCR Account Command

To configure an LCR account, enter the following command:

```
> config lcr accounts
```

Table 81 describes the parameters of `config lcr accounts`.

Table 81. LCR Account Parameters

Parameter	Description
[dn]	Phone number of the account.
type	Signaling protocol used by the endpoint (**SIP** | **MGCP**).
id	ID of the SIP or MGCP endpoint.

LCR Account Example

This example creates an entry as follows:

Phone number (the four digits required to connect to a local office telephone)**:** 5555
SIP ID: `nortel.five`

```
> config lcr accounts 5555 type SIP id nortel.five
*> save
```

Show LCR Accounts

To show the LCR accounts, enter the following command:

```
> show lcr accounts

LCR Accounts:
DN                    Type       ID
-------------------------------------------------------------
2222                  SIP        nortel.two
4444                  SIP        nortel.four
5555                  SIP        nortel.five
```

LCR Settings

You can configure the following LCR settings:

- The **gateway** that the device uses in LCR mode. The options are:
  - **INT**: external calls are routed through the Integrated Gateway through the FXO port and the PSTN (assuming that the FXO port is connected to a central office line).
  - **LGW**: external calls are routed through a SIP/PSTN gateway located on the LAN.

  A SIP/PSTN gateway can handle multiple, active calls, whereas the FXO port can handle only one active call at a time.

Note: MGCP gateways are not supported.

- The **emergency call number**. Calls to this number are given special treatment:
  - In LCR mode, emergency calls are established through the FXO port.
  - In connected mode, emergency calls are established through the WAN port with the maximum voice bandwidth allocated even if it affects the quality of existing voice calls.
- The **numbering plan** settings that allow the device to determine if the call is local or external. Specify the parameters `obaccess`, `areacode`, `coprefix`, and `enlength` to accurately reflect the numbering plan; the settings help identify a telephone number as a local endpoint. For a numbering plan example, see "Example: Local Numbering Plan" (page 259).

LCR Settings Command

To configure LCR settings, enter the following command:

```
> config lcr settings
```

Table 82 describes the parameters of `config lcr settings`.

Table 82. LCR Configuration Parameters

Parameter	Description
lcbmode	Local call backup mode (**INT** for the Integrated Gateway [the FXO port] or **LGW** for a SIP/PSTN gateway on the LAN). You can only configure one gateway. The default is **INT**.
ecnumber	Emergency call number. The default is **911**.
obaccess	Outbound access prefix digit such as 9 to place an outside call, as in 9-555-121). Applies only to hosted PBX service. The default is **9**.
areacode	Area code of this installation, such as, 408 in the phone number (408) 555-1001.
coprefix	Central office prefix of this installation, such as, 555 in the phone number (408) 555-1001.
enlength	Extension number length, such as, 4 for the last four digits in the number (408) 555-1001. The default is **4**.

Example: Emergency Calls over FxO Port

The following example designates the FXO port as the PSTN gateway for LCR mode and specifies the emergency call number as 911:

```
> config lcr settings lcbmode INT ecnumber 911
*> save
```

Example: Local Numbering Plan

The following example defines the local numbering plan as follows:

prefix for outbound calls: 9
area code: 408
central office prefix: 555
length of extension number: 4

```
> config lcr settings obaccess 9 areacode 408 coprefix 555
enlength 4
*> save
```

This configuration supports calls as follows:

Number dialed	Action
2210	Four-digit call so only local accounts are checked.
9411	Outbound prefix so number is interpreted as outbound call for 411.
95552210	Outbound prefix, but also central office prefix, so only local accounts are checked for 2210.
96872210	Outbound prefix, but not central office prefix, so route 6872210 to PSTN.
914085552210	Central office prefix so only local accounts are checked for 2210.
914086872210	No central office prefix so route 14086872210 to PSTN.

Show LCR Settings

To show the LCR settings, enter the following command:

```
> show lcr settings

LCR Settings:

LCBMode    ECNumber   OBAccess   AreaCode   COPrefix   ENLength
-----------------------------------------------------------
INT        911        9          408        555        4
```

FxO Gain and Impedance Settings

You can change telephony settings for DSP gain and impedance, as needed, for the FxO port.

DSP Gain Settings

To set the DSP gain values for the FxO port, enter the following command:

```
> config voice fxo gain
```

This commands parameters are as follows:

Parameter	Description
tx	Transmit (tx) gain (digital to analog conversion) in decibels. Specify a minus (-) before a negative value. The default is **0** dB.
rx	Receive (rx) gain (analog to digital conversion) in decibels. Specify a minus (-) before a negative value. The default is **0** dB.

Show Gain Settings

To show the DSP gain settings, enter the following command:

```
> show voice fxo gain

FXO Gain Global Settings:

   Tx      -0 dB
   Rx      -0 dB
```

FxO Line Impedance Settings

FxO line impedance settings are provided to reduce near-end echo and achieve the best voice quality for a certain country or market. For supported countries, the appropriate impedance settings are automatically set according to the country code (see “Country Code and Unit Name Setting” (page 239)). For those countries, the impedance setting remains the default, **automatic**.

Explicit impedance settings can be needed for a country or market without a supported country code. The impedance can be specified by the impedance parameter or by the AC impedance register and hybrid filter parameters. Together, the AC impedance register and hybrid filter settings constitute an impedance setting; you can modify them to customize and fine-tune the line impedance.

To set line impedance values for the FxO port, enter the following command:

```
> config voice fxo hw
```

This commands parameters are as follows:

Parameter	Description
impedance	Specialized impedance override setting for the line (automatic | 600 | 900 | 600_1uF | 900_2.16uF | 270+750_150nF | 220+820_120nF | 220+820_115nF | 200+680_100nF). The default is **automatic**.
acim	AC impedance register (customizing impedance only). The value refers to an AC line termination, as listed in Table 83. The default value is **11** (600 Ohms (Ω) + 2.16 µF).

Parameter	Description
hyb*n*, where *n* = 1-8	Hybrid filter *n* (1 - 8). Eight hybrid filters are provided (for customizing impedance only). Their allowed values are 0 - 255. The default value for each filter is **0**.

Table 83. AC Impedance Register Values

acim Value	AC Line Termination
0	600 Ω
1	900 Ω
2	270 Ω + (750 Ω || 150 nF) and 275 Ω + (780 Ω || 150 nF)
3	220 Ω + (820 Ω || 120 nF) and 220 Ω + (820 Ω || 115 nF)
4	370 Ω + (620 Ω || 310 nF)
5	320 Ω + (1050 Ω || 230 nF)
6	370 Ω + (820 Ω || 110 nF)
7	275 Ω + (780 Ω || 150 nF)
8	120 Ω + (820 Ω || 110 nF)
9	350 Ω + (1000 Ω || 210 nF)
10	0 Ω + (900 Ω || 30 nF)
11	600 Ω + 2.16 µF
12	900 Ω + 1 µF
13	900 Ω + 2.16 µF
14	600 Ω + 1 µF
15	Global complex impedance

Show FxO Impedance Settings

To show the impedance settings, enter the following command:

```
> show voice fxo hw

FXO Global HW Settings:

   Impedance     Automatic
   ACIM          11
   HYB1          0
```

```
HYB2          0
HYB3          0
HYB4          0
HYB5          0
HYB6          0
HYB7          0
HYB8          0
```

Show LCR Status

The session controller runs either in normal mode (all calls are established through a VoIP server) or in LCR mode (the BSGX4e device provides limited local and PSTN call service).

To see whether the session controller is running in LCR mode, enter the status command for the session controller. For example, this command shows the status of the SIP session controller:

```
> show sip sc status

SIP Session Controller status:

   SSC Started          Yes
   SSC Server Ready     No
   My Wan IpAddr        0.0.0.0
   Wan Rx Port          5060
   Lan Rx Port          5060
   CAC Max Calls        500
```

When the session controller runs in LCR mode, the **SSC Server Ready** line reports **No.**

Show LCR Connections

To show the connections established in LCR mode, enter the following command:

```
> show lcr connection

Connection List:

Caller              Called              To              Type
-------------------------------------------------------------
nortel.two            nortel.five       5555            Internal
```

The Type field reports if the connection is between two LAN endpoints or between a LAN endpoint and the PSTN. Note that a LAN endpoint can also be an analog device (through an FXS port and the Integrated Gateway).

15
SIP CONFIGURATION

This chapter describes the configuration of the SIP session controller and the SIP gateway. You can configure the BSGX4e device to act as both VoIP session controller and VoIP gateway. The session controller and VoIP gateway can use either the Session Initiation Protocol (SIP) or the Media Gateway Control Protocol (MGCP).

Configuration for MGCP is described in "MGCP Configuration" (page 209). VoIP topics that apply to both signaling protocols (SIP and MGCP) are discussed in "VoIP Configuration" (page 229).

Introduction to SIP

The Session Initiation Protocol (SIP) session controller controls the establishment and termination of VoIP sessions, as requested by endpoint devices. The integrated SIP gateway, which operates together with the session controller, serves as the VoIP gateway for analog devices.

Figure 17 shows a SIP network. In the figure, the BSGX4e device controls VoIP sessions for its LAN devices, which can be SIP phones and PC terminals. The BSGX4e device can also control VoIP sessions for an analog device (fax machine or phone) connected to an analog devices FXS port. To do so, the analog device requires access through the WAN to one or more SIP proxy servers and to one DNS server.

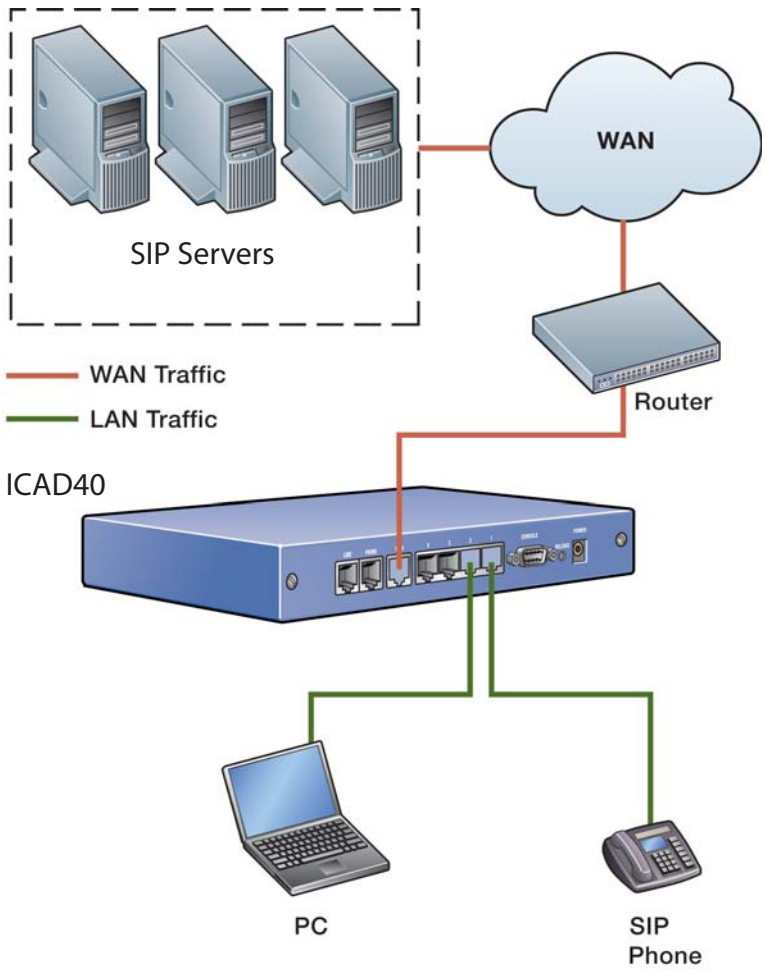


Figure 17. SIP Network Layout

SIP Session Controller

All VoIP traffic is directed through the session controller, which isolates and controls all VoIP devices on the internal network (LAN). The session controller can handle up to 1000 VoIP endpoints and up to 500 concurrent calls.

The session controller provides the following services:

- Serves as the interface between SIP endpoints and the SIP call server on the WAN. It interprets and relays all messages between the call server and the SIP devices on the LAN.
- Modifies Session Description Protocol (SDP) information to accommodate direct media connections and bridged connections (from LAN endpoint to LAN endpoint and from LAN endpoint to an endpoint on the WAN). This service is described in "Media Bridge (MBR)" (page 229).

- Monitors the registration status of the SIP endpoints on its LAN and times out the endpoint entry if the device becomes unregistered. The SIP registration information is kept in nonvolatile storage, so it can be immediately restored at restart.
- Manages the Access List Control (ACL) rules. Registration and call requests are accepted or rejected as directed by ACL rules. See "Access Control List (ACL)" (page 232).
- Rejects call requests if the internal endpoint is not registered.
- Rejects call requests if the WAN bandwidth required for the call is not available. See "Call Admission Control (CAC)" (page 236).
- Monitors voice quality. See "Voice Quality Monitoring (VQM)" (page 247).

The SIP session controller supports the following features:

- *Call server failover*: if the current SIP call server becomes unavailable, the session controller can switch service to an alternative call server.
- *Local call routing*: when VoIP service is unavailable, the SIP session controller still routes local calls within the LAN. It can also, optionally, route external calls to the PSTN network. See "Local Call Routing" (page 255).

SIP Gateway

The FXS port of the BSGX4e device can provide VoIP communication capabilities for an analog device. To do so, you must configure the integrated SIP gateway (also known as the SIP user agent). The SIP gateway interfaces VoIP to plain old telephone service (POTS) and connects an analog device (phone, modem, or fax machine) to the SIP network.

SIP Gateway Features

The SIP gateway supports the following features:

- Local dial plan and number analysis
- Do-not-disturb
- Forward-all
- Forward-on-busy
- Forward-no-answer
- Third-party call control

SIP Configuration Steps

The SIP configuration steps are:

1. **Configure access to one or more SIP call servers.**
2. **Configure the SIP session controller.**
3. **Configure SIP telephones, including the SIP gateway.**

SIP Call Server Access

This section describes how to configure a server profile, which determines how the session controller accesses SIP proxy servers to provide VoIP service.

One of the session controller settings specifies the call server profile that the session controller is to use. A server profile can explicitly specify up to three SIP proxy servers or it can specify no servers. If no server is explicitly specified, the session controller locates a SIP proxy server by using DNS SRV (as defined by RFC 2782 and RFC 3263).

NOTE: If the SIP server is to be found by DNS, you must configure the DNS client. Refer to "DNS Client" (page 50).

NOTE: The firewall is automatically updated to accept SIP messages from each SIP server specified or located.

Call Server Failover

Call server failover prevents VoIP service interruption by providing backup call servers. Call server failover is available only if the server profile used by the session controller explicitly specifies more than one SIP proxy server. Then, if the current SIP proxy server becomes unavailable, the session controller can reference the next SIP server in the profile.

The session controller detects that the call server might be down if it:

- cannot connect to it (for example, if the WAN interface is unplugged, or if an IP route is not available)
- does not receive SIP replies from it.

When the session controller detects that a server might be down, it attempts a number of retries before it marks the server as down. (The server profile specifies the number of retries.)

If the server is still unavailable after the retries, it is marked as down for the duration of the *blacklist* timer. (The server profile specifies the blacklist timer duration.) When the timer expires for a downed server, the session controller attempts to recontact the downed server.

While a SIP proxy server is marked as down, the session controller uses the next available SIP server. When a higher-priority server becomes available, the session controller switches back to the higher-priority server.

The session controller cannot establish SIP calls if the current SIP call server goes down and no other SIP server is available. In this case, the session controller repeatedly attempts to reconnect to the server and resumes call service as soon as the server comes back up. The availability of a second or third SIP server allows the session controller to use failover and avoid interrupting SIP phone service.

Additional Inbound Servers

The SIP session controller can accept inbound messages from additional SIP servers if those servers are explicitly specified in the server profile currently in use.

The firewall is automatically updated to accept SIP messages from the additional inbound servers.

You must specify the additional SIP servers by IP address in the SIP server profile. You can specify a single IP address or a range of addresses on the *ibserver1*, *ibserver2,* and *ibserver3* parameters.

SIP Server Profile Command

To configure a SIP server profile, enter the following command:

```
> config sip server settings
```

Table 84 describes the parameters for **config sip server settings.**

Table 84. SIP Server Profile Parameters

Parameter	Description
[name]	Name of the server profile to be created or edited.
domain	Registrar domain for registering SIP phones (FQDN | IP address). This parameter is required.
proxy1	First SIP proxy server (either a fully qualified domain name [FQDN] or an IP address). If you do not specify a proxy server, the session controller uses DNS to find its proxy servers.
port1	Port number of the first proxy server. The default is **5060**.
proxy2	Optional second SIP proxy server (FQDN | IP address).
port2	Port number of the second proxy server. The default is **5060**.
proxy3	Optional third SIP proxy server (FQDN | IP address).
port3	Port number of the third proxy server. The default is **5060**.
ibserver1	Optional additional inbound servers (IP address or range). The firewall is automatically updated to allow the session control to receive SIP messages from these additional servers.
ibserver2	Optional additional inbound servers (IP address or range).
ibserver3	Optional additional inbound servers (IP address or range).
retries	Number of retries before a SIP proxy server is blacklisted. The default is **4** retries. (Specifying **0** disables call server failover.)
blacklist	Blacklist timer in seconds. The default is **600** seconds (ten minutes).

SIP Server Profile Examples

The following examples define SIP server profiles. The session controller setting determines which server profile is used.

The first two examples show the two methods of setting the SIP server: explicitly or through DNS. All examples specify the registrar domain to be used for SIP service.

Example Using DNS to Locate the Server

The SIP session controller uses DNS to locate a SIP proxy server only if the parameters **proxy1**, **proxy2,** and **proxy3** are blank. (To clear the proxy parameter values, specify **no proxy1 no proxy2 no proxy3**.)

This example configures the SIP server automatically:

Setting name: EMM_Automatic
Registrar domain: emm.live.ericsson.net

```
> config sip server settings EMM_Automatic domain
emm.live.ericsson.net no proxy1 no proxy2 no proxy3
*> save
```

DNS updates the server settings as follows, depending on the priority it assigns to each SIP server:

- **proxy1** is assigned the SIP server of highest priority.
- **proxy2** is assigned the SIP server of medium priority.
- **proxy3** is assigned the SIP server of lowest priority.

Example that Explicitly Sets the Server

This example configures a single SIP server manually:

Setting name: EMM_Manual
Registrar domain: emm.live.ericsson.net
Proxy server: pcscf.emm.live.ericsson.net
Proxy server port: 6666

```
> config sip server settings EMM_Manual domain
emm.live.ericsson.net proxy1 pcscf.emm.live.ericsson.net
port1 6666
*> save
```

Example that Specifies a Backup Server

Up to three SIP proxy servers can be explicitly specified in a setting. The second server is used only if the first server is unavailable; the third server is used only if the first and second servers are unavailable.

This example configures a setting for failover mode:

Setting name: EMM_FailOverMode
Registrar domain: emm.live.ericsson.net
Proxy1: primary.emm.live.ericsson.net
Port1: 6666
Proxy2: secondary.emm.live.ericsson.net
Port2: 6666
Retries: 4
Blacklist: 300

```
> config sip server settings EMM_FailOverMode domain
emm.live.ericsson.net proxy1 primary.emm.live.ericsson.net
port1 6666 proxy2 secondary.emm.live.ericsson.net port2 6666
retries 4 blacklist 300
*> save
```

Example Specifying an Additional SIP Inbound Server

This example configures an additional inbound SIP server:

Setting name: `EMM_AdditionalServer`
Registrar domain: `emm.live.ericsson.net`
Proxy server: `pcscf.emm.live.ericsson.net`
Proxy server port: `6666`
Address of an additional SIP server: `192.168.134.100`

```
> config sip server settings EMM_AdditionalServer domain
emm.live.ericsson.net proxy1 pcscf.emm.live.ericsson.net
port1 6666 ibserver1 192.168.134.100
*> save
```

Show SIP Server Settings

To show the SIP server settings, enter the following command:

```
> show sip server settings

SIP Server "EMM_Manual":

   Name          EMM_Manual
   Domain        emm.live.ericsson.net
   Proxy1        pcscf.emm.live.ericsson.net
   Port1         6666
   Proxy2
   Port2         5060
   Proxy3
   Port3         5060
   IBServer1
   IBServer2
   IBServer3
   Retries       4
   Blacklist     600 sec

SIP Server "EMM_Automatic":

   Name          EMM_Automatic
   Domain        emm.live.ericsson.net
   Proxy1
   Port1         5060
   Proxy2
   Port2         5060
   Proxy3
```

```
   Port3         5060
   IBServer1
   IBServer2
   IBServer3
   Retries       4
   Blacklist     600 sec

SIP Server "EMM_FailOverMode":

   Name          EMM_FailOverMode
   Domain        emm.live.ericsson.net
   Proxy1        primary.emm.live.ericsson.net
   Port1         6666
   Proxy2        secondary.emm.live.ericsson.net
   Port2         6666
   Proxy3
   Port3         5060
   IBServer1
   IBServer2
   IBServer3
   Retries       4
   Blacklist     300 sec

SIP Server "EMM_AdditionalServer":

   Name          EMM_AdditionalServer
   Domain        emm.live.ericsson.net
   Proxy1        pcscf.emm.live.ericsson.net
   Port1         5060
   Proxy2
   Port2         5060
   Proxy3
   Port3         5060
   IBServer1     192.168.134.100
   IBServer2
   IBServer3
   Retries       4
   Blacklist     600 sec
```

Delete SIP Server Profile

To delete a SIP server profile, specify its name on the command **del sip server settings**. For example, the following command deletes the profile *EMM_Manual*:

```
> del sip server settings EMM_Manual
```

Show SIP Server Status

The session controller setting determines which server profile is used. (The profile name is specified by the **server** parameter on the **config sip sc settings** command.) To see the server profile currently in use, enter the following command:

```
> show sip server status

SIP Server "Example":

   Name          Example
   Active        Yes
   Mode          DNS-SRV
   Domain        emm.live.ericsson.net
   Proxy1        proxy1.emm.live.ericsson.net (In-use)
   Port1         6666
   Proxy2        proxy1.emm.live.ericsson.net (Ready)
   Port2         6666
   Proxy3
   Port3         0
   IBServer1
   IBServer2
   IBServer3
```

The display shows the information specified by the profile. It also shows the following status information:

Field	Description
Active	Yes: This server profile is in use.
Mode	DNS-SRV: DNS locates the proxies. Manual: The proxy servers are specified explicitly.
Proxy1, Proxy2, Proxy3	(In-use): This proxy is currently in use. (Ready): This proxy is available, but is not currently in use. (Down): This proxy is not available.

SIP Session Controller

The SIP session controller provides the following features:

Feature	Description	Configuration Command
SIP Signaling Proxy (SSP)	Relays SIP messages between SIP endpoints and SIP servers.	**config sip sc settings** (see "Session Controller Setting Command" (page 272)).
Media Bridge (MBR)	Controls how VoIP media traffic is established.	**config media settings** (see "Media Bridge (MBR)" (page 229)).
Access Control List (ACL)	Controls which LAN endpoints can place and receive calls.	**config voice acl** (see "Access Control List (ACL)" (page 232)).

Feature	Description	Configuration Command
Endpoint Status Handling (ESH)	Enables and disables LAN endpoints.	See "Endpoint Status Handling (ESH)" (page 277).
Call Admission Control (CAC)	Controls whether a call can be placed or received.	See "Call Admission Control (CAC)" (page 236).
Voice Quality Monitoring (VQM)	Reports the quality of calls.	**config calls analyzer** (see "Voice Quality Monitoring (VQM)" (page 247)).

SIP Signaling Proxy (SSP)

The SIP Signaling Proxy (SSP) relays SIP messages between SIP endpoints (phones or terminals) and a SIP proxy server on the WAN.

The session controller settings are:

- **server, lcdomain:** information for modifying SIP headers, so messages can be relayed.
- **wanrxport**, **lanrxport**: ports on which to listen for SIP signaling messages on the WAN and LAN, respectively.
- **timert1, timert2:** timeout intervals for SIP messages retransmission.
- **timerb, timerf, timerc**: timeout intervals for SIP transactions.
- **maxcalls**: maximum number of simultaneous SIP calls.
- **sigqos:** GoS quality group to protect SIP signaling from other traffic. SIP signaling traffic is sensitive to packet loss; if SIP packets are dropped, calls can fail.

Configuration Prerequisites

You must configure a server profile before you can specify a server profile for use by the session controller. See "SIP Call Server Access" (page 266).

To protect the quality of service for SIP signaling traffic, a session controller setting assigns SIP signaling traffic to a GoS quality group. You must configure the quality group before it can be specified as a session controller setting. For more information, see "GoS Configuration" (page 181).

Session Controller Setting Command

To configure the SIP session controller, enter the following command:

```
> config sip sc settings
```

Table 85 describes the parameters for **config sip sc settings**.

Table 85. SIP Session Controller Parameters

Parameter	Description
server	Name of the SIP call server setting to be used. To see the configured server profiles, enter **show sip server settings**.
lcdomain	Local domain for LAN endpoints. SIP messages that do not match the domain are discarded.
wanrxport	Port on which to listen for SIP signaling messages from the WAN. The default is **5060**.
lanrxport	Port on which to listen for SIP signaling messages from the LAN. The default is **5060**.
timert1	Minimum retransmission time interval (in milliseconds). The default is **500** milliseconds.
timert2	Maximum retransmission time interval (in milliseconds). The default is **4000** milliseconds.
timerb	Timeout interval for INVITE transactions (in seconds). The default is **16** seconds.
timerf	Timeout interval for non-INVITE transactions (in seconds). The default is **32** seconds.
timerc	Timeout interval for proxy INVITE transactions (in seconds). The default is **180** seconds (3 minutes).
maxcalls	Maximum number of SIP calls allowed simultaneously. The default is the maximum for the unit—**500** calls.
sigqos	Name of the GoS quality group that specifies the QoS protection for SIP signaling traffic. To see the configured quality groups, enter **show qos group**.

SIP Session Controller Setting Example

This example configures the SIP session controller as follows:

Name of the SIP server profile: `EMM`
WAN RX port: `5060`
LAN RX port: `5060`
GoS quality group to protect SIP signaling traffic: `VoIP`

```
> config sip sc settings server EMM wanrxport 5060 lanrxport
5060 sigqos VoIP
*> save
```

Show SIP Session Controller Settings

To show the SIP session controller settings, enter the following command:

```
> show sip sc settings

SIP Session Controller settings:
```

```
Server                  EMM
Local Domain
Wan Rx Port             5060
Lan Rx Port             5060
Timer T1                500 msec
Timer T2                4000 msec
Timer B                 16 sec
Timer F                 32 sec
Timer C                 180 sec
Max Calls               500
Signaling QoS Group     VoIP
```

Show SIP Session Controller Status

To show the status of the SIP session controller, enter the following command:

```
> show sip sc status
SIP Session Controller status:

   SSC Started          Yes
   SSC Server Ready     Yes
   My Wan IpAddr        172.29.250.5
   Wan Rx Port          5060
   Lan Rx Port          5060
   CAC Max Calls        500
```

The display shows configured information and the following status field:

- `SSC Server Ready Yes` if a SIP server is active.
  `No` if no SIP server is active.

Show SIP Signaling Statistics

The following command displays the statistics of the relayed SIP signaling packets:

```
> stats sip sc status

SIP Session Controller message stats:

   Msg per sec. (current/highest):      0/0

   TotalMsgRxCount                    200

   RxMsgDropSrcErr                      0
   RxMsgDropIntErr                      0
   RxMsgDropNoBufErr                    0
   RxMsgDropWanCsErr                    0
   RxMsgDropWanIfErr                    0
   TxMsgDropNoBufErr                    0
   TxMsgDropIntErr                      0
```

```
WanMsgRecvCount                    100
WanMsgProcCount                    100

WanMsgDropDataErr                    0
WanMsgDropNoBufErr                   0
WanReqCacRejErr                      0
WanReqDropSecFail                    0
WanReqDropDataErr                    0
WanRspDropDataErr                    0
WanRspDropStateErr                   0

LanMsgRecvCount                    100
LanMsgProcCount                    100

LanMsgDropDataErr                    0
LanMsgDropSecErr                     0
LanMsgDropNoBufErr                   0
LanReqEacRejErr                      0
LanReqCacRejErr                      0
LanReqDropSecFail                    0
LanReqDropDataErr                    0
LanRspDropDataErr                    0
LanRspDropStateErr                   0
```

The count fields (`WanMsgRecvCount`, `WanMsgProcCount`, `LanMsgRecvCount`, and `LanMsgProcCount`) report the counts of normal packets received and processed. The other fields report error counts.

Show SIP Call Statistics

The following command displays statistics for SIP calls:

```
> stats sip sc calls

SIP Session Controller signaling stats:

  Call per sec. (current/highest):         0/1

  Active calls (current/highest):          0/1

  Total calls attempted:                   7

     Total outbound calls from LAN:        6
        Calls on going:                    0
        Calls succeeded:                   6
        Calls failed:                      0
        - Call rejected no bandwidth:      0
        - Call cancelled:                  0
        - Call redirected:                 0
        - Call forbidden:                  0
        - Call not found:                  0
```

```
      - Called dest busy:                0
      - Others causes:                   0

   Total inbound calls from WAN:         1
      Calls on going:                    0
      Calls succeeded:                   0
      Calls failed:                      1
      - Call rejected no bandwidth:      0
      - Call cancelled:                  1
      - Call redirected:                 0
      - Call forbidden:                  0
      - Call not found:                  0
      - Called dest busy:                0
      - Others causes:                   0
```

The first section, `Total outbound calls from LAN`, applies to calls that originate from LAN endpoints. The second section, `Total inbound calls from WAN`, applies to calls that originate from the SIP server.

NOTE: A local call from a LAN endpoint to another LAN endpoint is shown twice in the statistics; it is counted both as a LAN outbound call and as a WAN inbound call.

Show SIP Call Records

A call record is kept for every call as shown in "Show Call History" (page 254). The SIP session controller also records detailed information about each SIP call. The following command displays SIP call entries:

```
> show sip sc calls

SIP Session Controller detailed call entries:

EP CallInfo         Call to:  4945
   EP Info          nortel.two, 10.0.20.2:5060
   Line State       CALL_ANSWER_ACKED
   Wan ToTag        2079605163-1140867899608
   Wan FromTag      3-25-85680fc8-00005af2
   Wan CallID       3-25-85680fc8-00001e5c@172.29.250.5
   Lan ToTag        3-25-85680fc8-00007b76
   Lan FromTag      000f8f07308800076d578d1c-7d53b8e2
   Lan CallID       000f8f07-30880004-51dee830-20cc6f3b@10.0.20.2
   Media Mode       NORMAL
   Media Type       AUDIO
   Media Conn_b     172.29.250.30:29490--172.29.250.5:13006<==
   Media Conn_a           ==>10.0.1.1:13006--10.0.20.2:29268
```

Show Registered Endpoints

To see a list of the LAN endpoints registered to the SIP server through the SIP session controller, enter the following command:

```
> show sip sc endpoints

SIP Session Controller endpoints:

Endpoint ID                EP Addr          EP Port          Act Calls
Endpoint Name              TelNo            Lan Domain       Timeout
-------------------------------------------------------------------------
nortel.two                   10.0.1.12        5060             1
4982                       nortel.two         10.0.1.1         1626
nortel.four                  127.0.0.1        5065             0
4984                       nortel.four        local            3578
nortel.five                  10.0.20.1        5060             0
4985                       nortel.five        10.0.1.1         1552
```

The configuration information in the display is the information stored when the endpoint is registered [see "Endpoint Status Handling (ESH)" (page 277)]. In addition, the display shows the following status fields:

- `Act Calls`
  This field shows the currently active calls for the endpoint. This field is incremented each time the LAN endpoint places or receives a call. This field is decremented when the call is torn down.
- `Timeout`
  This value represents the number of seconds before the registration expires. The initial value is taken from the **Expires** field of the SIP REGISTER method. The value is decremented each second.

Endpoint Status Handling (ESH)

Endpoint Status Handling (ESH) saves LAN endpoint information in nonvolatile memory, so it can be retrieved after a restart. This is done when the LAN endpoint is registered to the SIP server.

NOTE: ESH is not configurable for the SIP session controller.

The following information is stored:

- SIP endpoint ID
- IP address (see "IP Address Change" (page 289))
- SIP port
- Telephone number
- SIP domain
- Remaining active time (based on Expires field in the SIP REGISTER method)

The SIP session controller rejects calls that terminate at unregistered LAN endpoints. Thus, information about unregistered LAN endpoints is not stored, and any unregistered endpoint is not re-registered when the unit restarts.

SIP Gateway

The SIP gateway (also known as the user agent, or UA) is the software that allows an analog device such as a telephone or fax machine to use VoIP connections to place and receive calls. You must connect the analog device to the FXS port of the device as described in the installation guide.

This integrated SIP gateway is configured as if it is a VoIP SIP phone located on the LAN. The integrated SIP gateway currently supports the following features:

- Session timer
- Compressor-Decompressors (CODEC) G.711 u-law, G.711 a-law and G.729
- RFC 2833
- Modem pass-through
- Fax pass-through
- Multi-line support
- Voice Activation Detection (VAD)

Configuration Steps

Configuration of the SIP gateway requires the following steps:

1. Configure **SIP protocol settings** for the gateway (see "SIP Settings for the Gateway" (page 278)).
2. Configure **FXS port settings** (see "FXS Port Configuration" (page 238)).
3. Configure **SIP gateway settings** (see "SIP Gateway Configuration" (page 280)).
4. Configure the **numbering plan** for the analog device (see **"Numbering Plan for the Gateway" (page 284)**).

SIP Settings for the Gateway

This section describes the SIP protocol settings that apply to the SIP gateway.

NOTE: The SIP settings for the gateway do not apply to the SIP session controller.

You can modify the SIP protocol for interoperability purposes within the SIP environment. You can apply the following changes to the SIP protocol:

- Timeout intervals for the SIP timers (T1, T2, and B as defined in RFC 3261)
- Expiration time for the gateway registration
- Session timer support as defined in RFC 4028
- On-hold timer
- No-answer timer

NOTE: The SIP gateway attempts to register with the SIP server as soon as it is started; the SIP gateway cannot function until it is successfully registered.

SIP Gateway Settings Command

To configure the SIP protocol settings for the gateway, enter the following command:

```
> config sip ua settings
```

Table 86 describes the parameters for **config sip ua settings**.

Table 86. SIP Gateway Parameters

Parameter	Description
timert1	Minimum retransmission time interval (in milliseconds). The default is **500** milliseconds.
timert2	Maximum retransmission time interval (in milliseconds). The default is **4000** milliseconds.
timerb	Timeout interval for INVITE transactions (in milliseconds). The default is **32000** milliseconds.
regexpire	Timeout interval for expiration of the endpoint registration (in seconds). The default is **3600** seconds (1 hour).
seenable	Enables Session-Expires support (see **setimer** and **minsetimer**). The default is **no**.
setimer	Maximum session interval if no session refresh requests are received (in seconds). If the timer expires, the session ends. The default is **1800** seconds (30 minutes). This value is used only if **seenable** is **yes**.
minsetimer	Minimum session interval that the User Agent can accept (in seconds). The default is **90** seconds. This value is used only if **seenable** is **yes**.
onholdtimer	Maximum interval of time that the User Agent can be put on hold with no audio or music-on-hold (in seconds). If the on hold timer expires, the call is disconnected. The default is **180** seconds (3 minutes).
noanstimer	Maximum interval of time that the User Agent can be ringing without being answered (in seconds). If the no answer timer expires, the call is rejected with an assigned reason of either ring-timeout or call-forwarding on no answer (if the feature is enabled). The default is **60** seconds.

SIP Gateway Settings Example

This example configures the SIP settings for the gateway, as follows:

Session timer support: yes

MIN-SE timer: 500 seconds
Session expire timer: 600 seconds

```
> config sip ua settings seenable yes setimer 600 minsetimer
500
*> save
```

Show SIP Gateway Settings

To show the SIP settings for the gateway, enter the following command:

```
> show sip ua settings
SIP Protocol Settings:

   Timer T1                    500
   Timer T2                    4000 msec
   Timer B                     32000 msec
   RegExpire                   1800 sec
   SE Enable                   yes
   SE Timer                    600 sec
   MIN-SE Timer                500 sec
   On-Hold Timer               180 sec
   No-Answer Timer             60 sec
```

SIP Gateway Configuration

To configure the gateway, the following information is required:

- Authentication information required by the SIP server (user ID, authentication ID, and authentication password).
- The supported CODECs and the order they are proposed in negotiations.

  You can configure up to four CODECs. The supported CODECs are G.711 u-law, G.711 a-law, and G.729 with a 10ms or 20ms RTP packet interval.
- Feature activation for RFC 2833 for Dual-Tone Multi-Frequency (DTMF), modem pass-through, or fax pass-through.

  For a modem, you can configure the port to enable modem pass-through and force media to G.711 echo cancellation (**mpt on**).
  For a fax, you can configure the port:
  - to support fax pass-through and force media to G.711 echo cancellation (**fax on**)
  - to support fax pass-through and enable renegotiation of the CODEC with the remote party when a fax tone is detected **(fax auto**)

Configuration Restraints

- Before you configure the gateway, you must configure the SIP session controller, and the gateway settings for the SIP protocol and the FXS port. See “SIP Session Controller” (page 271), “SIP Settings for the Gateway” (page 278), and “FXS Port Configuration” (page 238).

- A codec parameter that is specified as **notused** acts as a terminator in the preferred codec list; subsequent codecs are ignored.

  For example, if the codec parameters are set as below, **codec3** and **codec4** are ignored; they are not proposed in negotiations:

  ```
  codec1 PCMU_10
  codec2 notused
  codec3 PCMU_20
  codec4 PCMA_20
  ```

- Currently, Fax T.38 is not supported.
- If the FXS port is configured as an MGCP gateway, you must delete that configuration before you can reconfigure the port as a SIP gateway.

SIP Gateway Configuration Command

To configure the SIP gateway, enter the following command:

```
> config sip ua port
```

Table 87 describes the parameters for **config sip ua port**.

Table 87. SIP Gateway Configuration Parameters

Parameter	Description
[port]	Number of the FXS port (**1**).
name	Name for the display.
userid	User ID of the SIP account. This parameter is required.
authid	Authentication ID of the SIP account.
password	Authentication password of the SIP account.
codec1	Most preferred codec and packet time selection (**PCMU_10** | **PCMU_20** | **PCMA_10** | **PCMA_20** | **G729A_10** | **G729A_20** | **NOTUSED**). The default is PCMU_20.
codec2	Second preferred codec and packet time selection (**PCMU_10** | **PCMU_20** | **PCMA_10** | **PCMA_20** | **G729A_10** | **G729A_20** | **NOTUSED**). The default is PCMA_20.
codec3	Third preferred codec and packet time selection (**PCMU_10** | **PCMU_20** | **PCMA_10** | **PCMA_20** | **G729A_10** | **G729A_20** | **NOTUSED**). The default is G729A_20.
codec4	Fourth preferred codec and packet time selection (**PCMU_10** | **PCMU_20** | **PCMA_10** | **PCMA_20** | **G729A_10** | **G729A_2**0 | **NOTUSED**). The default is NOTUSED.
rfc2833	Indicates whether to use RFC 2833 for DTMF (**yes** | **no**). (RFC 2833 provides *out of band DTMF* event reports.) The default is **yes**. Distortion from compression and decompression can prevent recognition of pure DTMF tones. Out-of-band DTMF sends the information by separate RTP packets.

Table 87. SIP Gateway Configuration Parameters (continued)

Parameter	Description
payload	If RFC 2833 is enabled (**rfc2833 yes**), you can specify the RTP dynamic payload type (96-127). The default is **101**.
mls	Feature currently not supported. (Enables multi-line support (**yes** | **no**). Specify **yes** if the FXS port is connected to a multi-line phone or Private Branch Exchange (PBX). The default is **no**.)
mpt	Enables modem pass-through and forces media to G.711 echo cancellation (**off** | **on**). Specify **on** if a modem is connected to the FXS port. The default is **off**.
fax	Enables fax pass-through and either forces media to G.711 echo cancellation (**on**) or enables renegotiation of the CODEC with the remote party when a fax tone is detected (**auto**). The default is **off**.
vad	Feature currently not supported. (Enables Voice Activity Detection (VAD) (silence suppression) (**yes** | **no**). The default is **no**. Enabling VAD allows the unit to conserve resources by avoiding sending silent RTP packets. However, VAD can silence very low sounds, lowering voice quality.)
up	Indicates whether the SIP gateway port is enabled (**yes** | **no**). The default is **yes**.

SIP Gateway Example

This example configures the SIP gateway for an analog telephone as follows:

Port: 1
Name: uap1
User ID: uap1
Authentication ID: uap1
Authentication password: mysecret
RFC2833 DTMF: yes
RFC2833 payload type: 96

```
> config sip ua port 1 name uap1 userid uap1 authid uap1
password mysecret rfc2833 yes payload 96
*> save
```

Show Gateway Configuration

To show the configuration of the SIP gateway, enter the following command:

```
> show sip ua port
SIP UA Ports:


Port  Name     AuthID    Codec1    Codec3     RFC2833 MLS Fax Running
      UserID   Password  Codec2    Codec4     Payload MPT VAD
```

```
-------------------------------------------------------------------
0-1  uap1    uap1      PCMU_20    G729A_20   yes    no  Off yes
     uap1              PCMA_20    NOTUSED    96     Off no
```

Delete SIP Gateway Configuration

To delete the SIP gateway configuration for the FXS port, enter the port number on a **del sip ua port** command. This allows for reconfiguration starting from default values; it is also required if the port is to be reconfigured as an MGCP gateway.

NOTE: A port currently in use cannot be deleted.

For example, the following command deletes the SIP gateway configuration for port 1:

```
> del sip ua port 1
```

Show SIP Gateway Status

To see the current status of the SIP gateway, enter the following command:

```
> show sip ua status

SIP UA Ports:

Port  RegStatus       Line 1               Line 2
-------------------------------------------------------------------
0-1   registered      Idle                 Idle
```

- The `RegStatus` field reports if the SIP gateway is correctly registered with the SIP server.
- The `Line 1` field (and `Line 2` field, if used) reports the status of the analog device:

`Idle`	The analog device is on-hook.
`OB (OutBound) Calling`	The analog device is off-hook or a phone number is being dialed.
`OB (OutBound) Proceeding`	The remote party is ringing.
`IB (InBound) Proceeding`	The analog device is ringing.
`Disconnecting`	The remote party is disconnected.
`Connected`	The analog device is in communication.

*NOTE: The Line 2 field is used when the multi-line support (**mls**) configuration option is selected.*

Show Media Stream Status

To see the current status of the VoIP media stream that terminates at the SIP gateway, enter the following command:

```
> show media stream
Media Stream
```

```
Chan  LocalNumber    CodecType  LocalConn            RtcpTx  RtpTx
Port  RemoteNumber   CodecState RemoteConn           RtcpRx  RtpRx
-------------------------------------------------------------------
5     1001           G711a      172.29.3.11:13008    0       0
0     2720           STARTED    172.29.11.120:16384  0       0
```

- The **LocalConn** and **RemoteConn** fields report the local and remote IP addresses and port numbers used by RTP for the connection.
- The **CodecType** and **CodecState** fields report the status of the media stream. In this example, the connection is started and uses the CODEC G.711 a-law.
- The **RtcpTx** and **RtcpRx** fields report the number of RTCP packets transmitted and received. The **RtpTx** and **RtpRx** fields report the number of RTP packets transmitted and received.

Numbering Plan for the Gateway

When an analog device, such as a phone, is connected to the FxS port, a numbering plan can be necessary to make full use of the features of the device. The SIP integrated gateway uses a numbering plan to interpret any string entered from the analog device.

The plan is a series of entries, each which defines how a specific string is to be interpreted. When the gateway receives a string from the analog device, it compares the string to the entries in the numbering plan and translates the string as needed before it is sent to the server.

- For service codes, the digits dialed are sent without modification.

  Note: Every service request entry must end with a hash character [#] to activate the service. For example, if the Do Not Disturb *code is set to *78, then an entry to activate* Do Not Disturb *for a phone is *78#.*

- For phone numbers, the string of digits can be translated as follows:
  - A number of digits can be stripped from the beginning of the number.
  - A string of digits can be prepended to the beginning of the number.

NOTE: Before you configure the numbering plan, you must configure the SIP gateway. See "SIP Gateway Configuration" (page 280).

Numbering Plan Command

To define an entry in the numbering plan, enter the following command:

```
> config voice np
```

Table 88 describes the parameters for **config voice np**.

Table 88. SIP Numbering Plan Parameters

Parameter	Description
[number]	String translated by the entry.

Table 88. SIP Numbering Plan Parameters (continued)

Parameter	Description
type	Indicates whether the entry is for a number or a service code (**number** | **service**).
feature	Feature type if *type* is **service**. It can be **None** or one of the following service codes: **SDND** Set Do Not Disturb (see "Do Not Disturb Example" (page 285)) **CDND** Clear Do Not Disturb **SFWA** Set Forward All (see "Call Forwarding Example" (page 286)) **CFWA** Clear Forward All **SFWB** Set Forward on Busy **CFWB** Clear Forward on Busy **SFWNA** Set Forward No Answer (see "Call Forwarding- No Answer Example" (page 286)) **CFWNA** Clear Forward No Answer **BXFER** Blind Transfer (see "Blind Transfer Example" (page 287))
length	Expected length of this number entry.
stripcount	Number of digits to strip off from the beginning of the number.
prepend	Digits to prepend to the beginning of the number.

Numbering Plan Entry Examples

The following are numbering plan entry examples.

Phone Number Prefix Example

This example configures a numbering plan entry to prepend a zero (0) to every phone number of length nine (9) that begins with a one (1). For example, if the phone number dialed is 123456789, the phone number called by the SIP gateway is 0123456789.

number: 1
type: number
length: 9
prepend: 0

```
> config voice np 1 type number length 9 prepend 0
*> save
```

Do Not Disturb Example

This example configures two numbering plan entries to enable the use of the *Do Not Disturb* feature:

- To set *Do Not Disturb* for a phone, the entry is ***78#**.
- To clear the *Do Not Disturb* state for a phone, the entry is ***79#**.

NOTE: The hash character (#) is required to activate a service entry.

Assuming these codes are processed by the SIP server, code *78 tells the SIP server to mark the SIP gateway as busy, so the server returns the appropriate error code if it is called. Code *79 tells the SIP server to release the SIP gateway from the busy state.

The parameters for the two numbering plan entries are:

number: *78
type: service
feature: SDND (Set Do Not Disturb**)**

number: *79
type: service
feature: CDND (Clear Do Not Disturb**)**

```
> config voice np *78 type service feature SDND
*> config voice np *79 type service feature CDND
*> save
```

Call Forwarding Example

This example configures two numbering plan entries to enable the use of the *Call Forwarding* feature:

- To forward calls to another phone, the entry is ***90**, followed by the phone number and the hash character (**#**). For example, to forward calls to phone 4985, the entry is ***904985#.**
- To clear call forwarding for a phone, the entry is ***91#**.

NOTE: The hash character (#) is required to activate a service entry.

The parameters for the two numbering plan entries are:

number: *90
type: service
feature: SFWA (Set Forward All**)**

number: *91
type: service
feature: CFWA (Clear Forward All**)**

```
> config voice np *90 type service feature SFWA
*> config voice np *91 type service feature CFWA
*> save
```

Call Forwarding- No Answer Example

The *Call Forwarding-No Answer* feature forwards calls from the phone only if the call is not answered before the *No Answer* timer expires.

NOTE: The duration of the **No Answer** *timer is a SIP gateway setting. The default is 60 seconds. See "SIP Gateway Settings Command" (page 279).*

This example configures two numbering plan entries to enable the use of the *Call Forwarding-No Answer* feature:

- To forward unanswered calls to another phone, the entry is ***93**, followed by the phone number and the hash character (**#**). For example, to forward unanswered calls to phone 4985, the entry is ***934985#.**
- To clear unanswered call forwarding for a phone, the entry is ***94#**.

NOTE: The hash character (#) is required to activate a service entry.

The parameters for the two numbering plan entries are:

number: *93
type: service
feature: SFWNA (Set Forward No Answer)

number: *94
type: service
feature: CFWNA (Clear Forward No Answer)

```
> config voice np *93 type service feature SFWNA
*> config voice np *94 type service feature CFWNA
*> save
```

Blind Transfer Example

This example configures the blind transfer (BXFER) feature. The blind transfer feature is used when a receptionist receives a call and the caller asks to speak to another employee. The receptionist then enters the blind transfer service code, the phone number of the other employee, and the hash character (#).

NOTE: The blind transfer (BXFER) feature is available only if the multi-line support (MLS) option is enabled for the SIP gateway (see "SIP Gateway Configuration Command" (page 281)).

For example, if the blind transfer service code is ***80**, the entry to transfer a call to phone number **4950**, is ***804950#**.

The following command configures ***80** as the service code for blind transfers (**BXFER**):

```
> config voice np *80 type service feature BXFER
*> save
```

Show Numbering Plan

To show the numbering plan, enter the following command:

```
> show voice np
Voice NP

Number              Type    Feature Length StripCount Prepend
-------------------------------------------------------------
```

```
*78                 Service SDND    0      0
*79                 Service CDND    0      0
*80                 Service BXFER   0      0
*90                 Service SFWA    0      0
*91                 Service CFWA    0      0
*93                 Service SFWNA   0      0
*94                 Service CFWNA   0      0
1                   Number  None    9      0          0
```

SIP Endpoints

This section provides guidelines to configure the SIP endpoints to be managed by the BSGX4e device.

To enable a SIP endpoint to place and receive calls, it must be:

- Allowed access by the Access Control List (ACL). See "Access Control List (ACL)" (page 232).
- Registered with the SIP server through the SIP session controller.

These requirements also apply to the SIP gateway because the SIP session controller handles the gateway as a SIP endpoint. However, unlike other endpoints, you cannot configure an ACL entry to disallow the SIP gateway. The ACL entry is automatically allowed to place and receive calls and cannot be disallowed.

Preparing Endpoints for Registration

The SIP endpoints need to be registered to the SIP server through the SIP session controller using the SIP method REGISTER. To be able to be registered, the SIP endpoints must be configured as follows:

- SIP registration must be enabled.
- The SIP proxy must be the LAN IP address of the BSGX4e device.
- The SIP proxy port must be the one configured as the LAN Rx port in the SIP session controller.
- No SIP outbound proxy is needed.
- NAT/firewall traversal must be disabled.
- The SIP domain must be the LAN IP address of the BSGX4e device.

For example, for a Cisco SIP phone 7960, firmware P0S3-07-5-00, the following configuration is required (interactive menu or text configuration file):

- **`proxy_register:`** 1 (enabled)
- **`proxy1_address:`** LAN IP address of the BSGX4e device
- **`proxy1_port:`** LAN Rx port of the SIP session controller
- **`outbound_proxy:`** blank
- **`nat_enabled:`** 0

- **domain:** LAN IP address of the BSGX4e device

Verify Endpoint Registration

To verify that the endpoints are correctly registered, enter the following command:

```
> show sip sc endpoints
SIP Session Controller endpoints:

Endpoint ID                EP Addr          EP Port          Act Calls
Endpoint Name              TelNo            Lan Domain       Timeout
-------------------------------------------------------------------
nortel.two                   10.0.1.12        5060             1
4982                       nortel.two         10.0.1.1         1626
nortel.four                  127.0.0.1         5065             1
nortel.four                  nortel.four        local            1697
```

The entry for the SIP gateway can be distinguished from the other endpoints because its `EP Addr` is set to the loopback IP address `127.0.0.1`.

IP Address Change

If the IP address of the BSGX4e device changes, all SIP registrations go stale and all VoIP services stop working. If this happens, all IP phones on the LAN must be rebooted and the SIP user agent for the FxS port must reregister.

To force the SIP agent to reregister, disable and reenable the FxS port. To do so, enter the following commands:

```
> config sip ua port all up no
> config sip ua port all up yes
```

For a complete description of the command, see "SIP Gateway Configuration Command" (page 281).

Configuring SIP

This section describes the steps for setting up the SIP Session Controller and SIP User Agent of the BSGX4e for use with LAN VoIP phones and an analog fax machine.

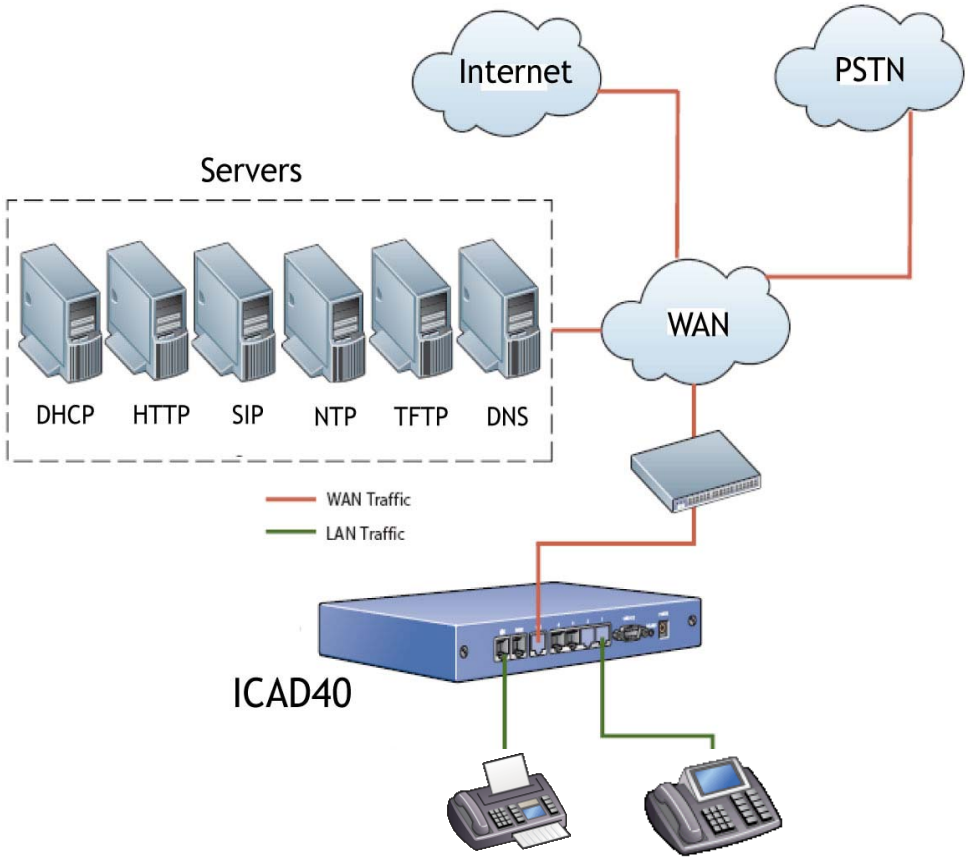


Table 89 describes network information, and Table 90 describes server information

Table 89. Network Information

LAN IP range Access router	10.0.0.0/16 10.0.1.1 (BSGX4e)
WAN range Access router	172.29.250.0/24 172.29.250.1

Table 90. Server Information

S1 DHCP Server	dhcpserver.isp.com - 66.19.9.160 (the access router acting as a DHCP relay between the BSGX4e and the DHCP server)
S2 HTTP Server	Httpserver.isp.com - 66.19.9.161
S3 SIP Server	Sipserver.com - 66.19.9.162 / SIP domain "sip.net"
S4 NTP Server	ttpserver.isp.com - 66.19.9.163
S5 TFTP Proxy	tftpserver.isp.com - 66.19.9.164
S6 DNS Server	dnsserver.isp.com - 66.19.9.165

This section provides guidelines for configuring the SIP Session Controller and the SIP User Agent of the BSGX4e. Configuration guidelines are given to describe an actual case for configuring an BSGX4e for deployment at a small customer office to implement a complete secure VoIP solution based on Cisco 7960 phones and a fax machine. The SIP Session Controller (SIP SC) controls the VoIP telephones installed in the LAN network. The SIP User Agent (SIP UA) controls the analog fax machine attached to the FXS port of the BSGX4e.

In this example the ISP managing the BSGX4e provides support services, including:

Dynamic Host Configuration Protocol (DHCP)	IP address management
Hypertext Transfer Protocol (HTTP)	VoIP phone logo management
Session Initiated Protocol (SIP)	Voice application
Simple Network Time Protocol (SNTP)	Time synchronization
Trivial File Transfer Protocol (TFTP)	VoIP phone firmware and configuration management
Domain Name Service (DNS)	SIP server location and name resolution

The first objective of the following example is to configure the SIP SC so that the LAN VoIP phones can connect and automatically do the following tasks:

1. Get an IP address.

2. **Upgrade their firmware if necessary.**
3. **Download a configuration file.**
4. **Get the clock time from the network.**
5. **Display a logo on their screen.**
6. **Register with the SIP server.**

The second objective is to configure the SIP UA so that the fax machine can make calls.

Once these two objectives are covered, this document shows the steps to configure a VoIP phone, check the overall configuration, and make calls. An annex at the end of this document provides the configuration for the IP phone (Cisco 7960) used in this example.

Step 1-Configure BSGX4e Session Controller

Configuration of the IP Network

1. Connecting to the network.
   Connect the Wide Area Network (WAN) port to the Internet Service Provider (ISP) router.
   Check that the WAN port Light Emitting Diode (LED) is green.

NOTE: If the LED is not green, check your physical installation.

2. **Configuring the WAN IP address of the unit.**
   The DHCP client must be on the WAN (eth0) interface of the BSGX4e.

```
bsg> config interface ip eth0 dhcp on
*bsg*> show interface ip eth0
"eth0" info:
   Interface            eth0
   Flags               (A843)<UP BROADCAST RUNNING SIMPLEX LINKUP MULTICAST>
   IP Address/Mask       172.29.250.5/255.255.255.0
   MTU                   1500
   DHCP                  on
   Lease obtained        SUN FEB 19 14:14:02 2006
   Lease expires         SUN FEB 19 15:14:02 2006
   MAC Address           00:40:00:05:00:00
   Speed                 FULL100
   Configured Speed      AUTONEG
```

NOTE: If the unit has not been assigned an IP address, the IP address field shows 0.0.0.0. Check your DHCP configuration.

3. **Configuring the default IP gateway.**
   The default IP gateway is automatically configured if the DHCP server provides a default gateway option. Otherwise, it must be manually configured.

```
*BSG*> config route table default gw 172.29.250.1
*BSG*> show route table
Destination      Netmask          Gateway          Interface
-------------------------------------------------------------------------
0.0.0.0          0.0.0.0          172.29.250.1     eth0
10.0.0.0         255.255.0.0      10.0.1.1         eth1
127.0.0.0        255.0.0.0        127.0.0.1        lo0
172.29.250.0     255.255.255.0    172.29.250.5     eth0
```

4. **Configuring the DNS client of the BSGX4e.**
   The DNS client is automatically configured if the DHCP server provides a DNS option. Otherwise, it must be manually configured.

```
*BSG*> config system dns dns1 66.19.9.165 domain wan.com
*BSG*> show system dns
DNS Settings:
   DNS1       66.19.9.165
   DNS2       0.0.0.0
   Domain     wan.com
```

5. **Check that all servers are reachable.**
   Ping the DNS server.

```
*BSG*> ping 66.19.9.165
Pinging 66.19.9.165 (66.19.9.165): 56 data bytes
Reply from 66.19.9.165: bytes=56 icmp_seq=0 time=190ms
Reply from 66.19.9.165: bytes=56 icmp_seq=1 time=180ms
Reply from 66.19.9.165: bytes=56 icmp_seq=2 time=170ms
Reply from 66.19.9.165: bytes=56 icmp_seq=3 time=200ms
----- 66.19.9.165 ping statistics -----
4 packets transmitted, 4 packets received, 0.0% packet loss
Round-trip times: min/avg/max=170/185/200ms
```

NOTE: If the ping fails, check your DNS configuration.

Ping the HTTP server.

```
*BSG*> ping httpserver.isp.com
Pinging httpserver.isp.com (66.19.9.161): 56 data bytes
Reply from 66.19.9.161: bytes=56 icmp_seq=0 time=190ms
Reply from 66.19.9.161: bytes=56 icmp_seq=1 time=180ms
Reply from 66.19.9.161: bytes=56 icmp_seq=2 time=170ms
Reply from 66.19.9.161: bytes=56 icmp_seq=3 time=200ms
----- httpserver.isp.com ping statistics -----
4 packets transmitted, 4 packets received, 0.0% packet loss
Round-trip times: min/avg/max=170/185/200ms
```

Ping the SIP server.

```
*BSG*> ping sipserver.isp.com
Pinging sipserver.isp.com (66.19.9.162): 56 data bytes
Reply from 66.19.9.162: bytes=56 icmp_seq=0 time=190ms
Reply from 66.19.9.162: bytes=56 icmp_seq=1 time=180ms
Reply from 66.19.9.162: bytes=56 icmp_seq=2 time=170ms
Reply from 66.19.9.162: bytes=56 icmp_seq=3 time=200ms
----- sipserver.isp.com ping statistics -----
4 packets transmitted, 4 packets received, 0.0% packet loss
Round-trip times: min/avg/max=170/185/200ms
```

Ping the SNTP server.

```
*BSG*> ping ntpserver.isp.com
Pinging ntpserver.isp.com (66.19.9.163): 56 data bytes
Reply from 66.19.9.163: bytes=56 icmp_seq=0 time=190ms
Reply from 66.19.9.163: bytes=56 icmp_seq=1 time=180ms
Reply from 66.19.9.163: bytes=56 icmp_seq=2 time=170ms
Reply from 66.19.9.163: bytes=56 icmp_seq=3 time=200ms
----- ntpserver.isp.com ping statistics -----
4 packets transmitted, 4 packets received, 0.0% packet loss
Round-trip times: min/avg/max=170/185/200ms
```

Ping the TFTP server.

```
*BSG*> ping tftpserver.isp.com
Pinging tftpserver.isp.com (66.19.9.164): 56 data bytes
Reply from 66.19.9.164: bytes=56 icmp_seq=0 time=190ms
Reply from 66.19.9.164: bytes=56 icmp_seq=1 time=180ms
Reply from 66.19.9.164: bytes=56 icmp_seq=2 time=170ms
Reply from 66.19.9.164: bytes=56 icmp_seq=3 time=200ms
----- tftpserver.isp.com ping statistics -----
4 packets transmitted, 4 packets received, 0.0% packet loss
Round-trip times: min/avg/max=170/185/200ms
```

NOTE: If any of these pings fails, check your server configuration.

6. **Configuring the SNTP client of the BSGX4e.**
   The SNTP client is automatically configured if the DHCP server provides an SNTP option. Otherwise, it must be manually configured, specifying the server and the Greenwich Mean Time (GMT) offset.

```
*BSG*> config system sntp enabled srv1 ntpserver.isp.com gmt +9
*BSG*> show system sntp
SNTP:
   Enabled          on
```

```
   Server 1          ntpserver.isp.com
   Server 2          0.0.0.0
   Server 3          0.0.0.0
   Server 4          0.0.0.0
   Gmt Offset        +09:00
   Sync Interval     7 days
   Last Sync         MON FEB 27 02:30:11 2006
   Next Sync         MON MAR 06 02:30:11 2006
*BSG*> time
MON FEB 27 02:30:25 2006
```

7. Configuring the LAN IP address of the unit.

Assign the IP address 10.0.1.1/16 to LAN interface eth1.

```
*BSG*> config interface eth1 ip 10.0.1.1/16
*BSG*> show interface ip eth1
"eth1" info:
Interface           eth1
  Flags              (A843) <UP BROADCAST RUNNING SIMPLEX LINKUP MULTICAST>
IP Address/Mask     10.0.1.1/255.255.0.0
MTU                 1500
DHCP                off
Lease obtained      N/A
Lease expires       N/A
MAC Address         00:40:00:05:00:01
Speed               N/A
Configured Speed    N/A
```

8. Configuring GoS (Layer 3 QoS) to protect VoIP traffic.

Configure a QoS link to manage outgoing traffic on the WAN port (eth0). The link bandwidth is 1 500 000 bps (1.5 Mbps, about T1 speed). For example:

```
*BSG*> config qos link eth0 max 1500000 comment T1Speed
*BSG*> show qos link
QoS Links:
Interface Max             Comment
-------------------------------------------------------------------------
 eth0      1500000       T1Speed
```

NOTE: The maximum rate specified takes into account the Ethernet header.

Configure a Quality Group to protect ten G.711 20 ms calls (Ethernet packet size 214 bytes without FCS, 50 packets/second). For the first nine calls, reserve 9 calls x 50 packets x 214 bytes x 8 bits = 770,400 bps. For the tenth call, reserve bandwidth for a G.711 10 ms call (1 call x 100 packets x 134 bytes x 8 bits = 107,200 bps). (This is the result of the Call Admission Control algorithm described in Annex B.)

Assign the Quality Group to the A1 quality class so it receives the highest priority (guaranteeing the lowest delay and loss). Use strict policing (policed) so traffic cannot be downgraded.

```
*BSG*> config qos group VoIP link eth0 qg A1 type policed committed 877600
```

```
*BSG*> show qos group
QoS Quality Groups:
Name            Link  QG    Type       Committed  Burst      IPToS COS
-------------------------------------------------------------------------
VoIP            eth0  A1    policed    877600     0          no    no
```

NOTE: The specified committed rate takes into account the Ethernet header.

NOTE: The other traffic types will be managed in Best Effort mode (for example, with higher delay or loss).

Data service configuration for the LAN VoIP phones: DHCP, SNTP, and TFTP

9. Configuring a DHCP server for the LAN VoIP phones.

Configure the DHCP server on the LAN interface (with subnet, netmask and broadcast addresses matching the eth1 configuration).

```
*BSG*> config dhcps pool eth1 subnet 10.0.0.0 netmask 255.255.0.0 ip
10.0.1.100-10.0.1.200
```

Configure the DHCP option for the default IP gateway (the LAN IP address of the BSGX4e).

```
*BSG*> config dhcps pool eth1 gateway 10.0.1.1
```

Configure the DHCP options for the services that the VoIP phones access (DNS, SNTP, and TFTP).

```
*BSG*> config dhcps pool eth1 dns1 10.0.1.1
*BSG*> config dhcps pool eth1 ntp1 10.0.1.1 gmtoffset +9
*BSG*> config dhcps pool eth1 tftp 10.0.1.1
*BSG*> config dhcps pool eth1 opt_150 10.0.1.1
```

NOTE: The TFTP server option for Cisco phones is 150.

NOTE: The VoIP phones must reach the LAN interface of the BSGX4e to access DNS, SNTP, and TFTP services. The BSGX4e then relays the requests to the servers and relays the replies to the originators (see next section).

Display the full configuration of the DHCP server.

```
*BSG*> show dhcps pool
DHCP Pools:
   Interface              eth1
   Subnet                 10.0.0.0
   Netmask                255.255.0.0
   IP                     10.0.1.100 - 10.0.1.200
   Broadcast              10.0.255.255
   Lease                  7 days
Options:
   Gateway                10.0.1.1
   DNS1                   10.0.1.1
   DNS2                   0.0.0.0
```

```
   TFTP                    10.0.1.1
   Filename
   Domain
   NTP1                    10.0.1.1
   NTP2                    0.0.0.0
   Timezone GMT Offset     +9 [hh:mm]
   150                     10.0.1.1
   151                     0.0.0.0
   160                     0.0.0.0
   161                     0.0.0.0
```

10. Configuring the relay functions for DNS, SNTP, and TFTP for LAN VoIP phones.

Configure the DNS relay so the BSGX4e relays DNS requests and replies between LAN VoIP phones and the DNS server located in the WAN.

```
*BSG*> config relay dns settings enabled yes dns1 66.19.9.165
*BSG*> show relay dns settings
DNS Relay Settings:
   Enabled     on
   DNS1        66.19.9.165
   DNS2        0.0.0.0
   DHCP        off
```

Configure the SNTP relay so the BSGX4e relays SNTP requests and replies between LAN VoIP phones and the NTP server located in the WAN.

```
*BSG*> config relay sntp settings enabled yes server ntpserver.isp.com
*BSG*> show relay sntp settings
SNTP Relay Settings:
   Enabled     on
   Server      ntpserver.isp.com
   DHCP        off
   GMT         0 hours
```

Configure the TFTP relay so the BSGX4e relays TFTP requests and replies between LAN VoIP phones and the TFTP server located in the WAN.

```
*BSG*> config relay tftp settings enabled yes server tftpserver.isp.com
*BSG*> show relay tftp settings
TFTP Relay Settings:
   Enabled      on
   Server       tftpserver.isp.com
   DHCP         off
   Allow        get
   Sessions     50
```

Configuration of the SIP voice services offered to LAN VoIP phones

11. Configuring the SIP server.

Configure the SIP server in automatic mode using DNS. The domain name for the SIP server location is sip.net.

```
*BSG*> config sip server settings SipProxy domain sip.net
*BSG*> show sip server settings
SIP Server "SipProxy":
   Name          SipProxy
   Domain        sip.net
   Proxy1
   Port1         5060
   Proxy2
   Port2         5060
   Proxy3
   Port3         5060
   IBServer1
   IBServer2
   IBServer3
   Retries       4
   Blacklist     600 sec
```

Display the results of the DNS-SRV process.

```
*BSG*> show sip server status
SIP Server "SipProxy":
   Name          SipProxy
   Active        Yes
   Mode          DNS-SRV
   Domain        sip.net
   Proxy1        sipserver.isp.com (In-use)
   Port1         6666
   Proxy2
   Port2         0
   Proxy3
   Port3         0
   IBServer1     0.0.0.0
   IBServer2     0.0.0.0
   IBServer3     0.0.0.0
```

If no proxy server is found (the proxy1 field is blank), check your DNS configuration.

12. Configuring the SIP Session Controller.

Configure the SIP SC to use the SIP server SipProxy, to receive and send SIP messages on port 5060 on both LAN and WAN, and to protect the signalling traffic according to the Quality Group VoIP.

```
*BSG*> config sip sc settings server SipProxy lanrxport 5060 wanrxport 5060
       sigqos VoIP
*BSG*> show sip sc settings
SIP Session Controller settings:
   Server                SipProxy
   Local Domain
   Wan Rx Port           5060
```

```
   Lan Rx Port             5060
   Timer T1                500 msec
   Timer T2                4000 msec
   Timer B                 16 sec
   Timer F                 32 sec
   Timer C                 180 sec
   Max Calls               500
   Signaling QoS Group     VoIP
```

13. Configuring Access List Control.

By default, all LAN VoIP phones are allowed to make calls.

```
*BSG*> show voice acl
Session Controller - ACL:
No policy matched counter: 0
Id Seq EpId     Platform IP               MAC Address               Action
       Software DeviceId                  Type                      Stats
-------------------------------------------------------------------------
1  1   any      any      any              any                       aBSGllow
       any      any                       any                      23
```

14. Configuring Call Admission Control.

Configure protection of media traffic according to Quality Group VoIP constraints. Call Admission Control prevents established calls from being disrupted if the Quality Group is oversubscribed. Because the Quality Group VoIP has been sized to protect ten G.711 calls, if an eleventh call tries to be established, Call Admission Control rejects the eleventh call due to insufficient bandwidth.

```
*BSG*> config media settings audioqos VoIP
*BSG*> show media settings
Media config:
   DM Enabled     No
   RTP Ports      13000 - 14999
   AudioQoS       VoIP
   MaxConn        500
```

Step 2-Configuring the BSGX4e User Agent

1. Configuring SIP User Agent.

The SIP User Agent is bound to the FXS port of the BSGX4e. This port is typically attached to a fax machine. Currently, the BSGX4e operates a fax machine on the IP network in G.711 Echo Cancellation mode.

```
BSG> config sip ua port 1 name Fax userid Fax authid Fax password Fax fax on
     up yes
*BSG*> show sip ua port 1
Port  Name   AuthID   Codec1   Codec3    RFC2833 MLS Fax       Running
      UserID Password Codec2   Codec4    Payload MPT VAD
```

```
-------------------------------------------------------------------------
0-1   Fax    Fax      PCMU_20  G729A_20  yes     no  On        Yes
      Fax    Fax      PCMA_20  NOTUSED   96      Off no
```

Step 3-Configure LAN VoIP phones (Example using Cisco 7960)

1. Preparing a LAN VoIP phone for data services.

DHCP must be enabled. DNS, SNTP, and TFTP server requests from the LAN phone must be configured to use the LAN IP address of the BSGX4e. The HTTP server must be set to httpserver.isp.com so the phone can retrieve a logo to display on its screen.
For a Cisco 7960 SIP phone, set parameters as follows: (A full configuration example is provided in Annex A.)

- dhcp: enable
- dns server 1: 10.0.1.1
- sntp_server: 10.0.1.1
- tftp_server: 10.0.1.1
- logo_url: http://httpserver.isp.com/usage/logo.bmp

2. Preparing a LAN VoIP phone for voice services.

The phone must be configured as follows:

- SIP registration must be enabled for an account. For example, for the account 1234, configure name: 1234, authentication ID: 1234, password: 1234.
- SIP proxy must be the LAN IP address of the BSGX4e.
- SIP proxy port must be the one configured for the SIP SC (its LAN Rx port).
- No SIP outbound proxy is needed.
- SIP domain must be the LAN IP address of the BSGX4e.
- NAT/Firewall traversal must be disabled.
  For a Cisco 7960 SIP phone, set parameters as follows: (A full configuration example is provided in Annex A.)
- proxy_register: 1 (line1_name: 1234, line1_authname: 1234, line1_password: 1234, phone_label: 1234, line1_displayname: 1234)
- proxy1_address: 10.0.1.1
- proxy1_port: 5060
- outbound_proxy: ""
- nat_enabled: 0
- SIP domain: 10.0.1.1

3. Connecting the VoIP phone to a LAN port of the BSGX4e.

The VoIP phone should:

- Get an IP address.
- Upgrade its firmware if necessary.
- Download a configuration file.
- Get the clock time from the network.
- Display a logo on its screen.
- Register with the SIP server.

Step 4-Check the overall configuration

1. Checking the status of the SIP UA.

Check that the SIP UA is correctly registered to the SIP server.

```
*BSG*> show sip ua status
SIP UA Ports:
Port  RegStatus       Line 1              Line 2
-------------------------------------------------------------------------
0-1   registered      Disconnecting       Idle
```

NOTE: The status registered means that the SIP UA is correctly registered to the SIP server. If any other status is shown, then the SIP UA is not registered and cannot work. If so, check your SIP configuration.

2. Checking that the LAN VoIP phone has an IP address assigned by the DHCP server.

```
"*BSG*> show dhcps lease
DHCP Leases:
IP              StartTime               Hostname
                EndTime                 MAC
-------------------------------------------------------------------------
10.0.1.100      2006/02/26 12:38:18     SIP000F8F073088
                2006/02/27 12:38:18     00:0f:8f:07:30:88
```

NOTE: If the LAN VoIP phone does not have an IP address, check the DHCP configuration.

3. Checking the status of the LAN SIP phone.

Check that the LAN SIP phone reports that it is registered on its screen.

NOTE: If the LAN SIP phone is not registered, check your SIP configuration.

4. Checking the status of the SIP SC.

Check that the SIP SC reports the SIP endpoints registered to the SIP server (SIP UA and LAN SIP phone).

```
BSG> show sip sc endpoints
SIP Session Controller endpoints:
Endpoint ID              EP Addr         EP Port         Act Calls
Endpoint Name            Phone Number    Lan Domain      Reg Timeout
-------------------------------------------------------------------------
1234                     10.0.1.100      5060            0
1234                     1234            10.0.1.1        1602
Fax                      127.0.0.1       5065            0
Fax                      fax             local           1600
```

NOTE: This display shows two entries: the LAN VoIP phone and the SIP UA. This shows that both are registered to the SIP server through the SIP SC.

Step 5-Make calls

1. The SIP UA is now ready to make a call. Making a fax call.

Check that the voice quality is correctly reported while the call is running.

```
BSG> show call current
Call List:
A Party    B Party    Type        Protocol        Start Time
A Number   B Number   State       Quality         Duration
-------------------------------------------------------------------------
Fax        OtherFax   Outbound    SIP             FEB 25 12:49:29 2006
Fax        OtherFax   Connected   4.20/4.18       10 seconds
```

2. The LAN VoIP phone is now ready to make a call. Making a phone call.

Check that the voice quality is correctly reported while the call is running.

```
BSG> show call current
Call List:
A Party    B Party    Type        Protocol        Start Time
A Number   B Number   State       Quality         Duration
-------------------------------------------------------------------------
1234       5678       Outbound    SIP             FEB 25 12:50:59 2006
1234       5678       Connected   4.20/4.18       21 seconds
```

Annex A-Configuration example for Cisco 7960 SIP phone

```
# SIP Default Configuration File
# Image Version
image_version: P0S3-07-5-00

# SIP Configuration Generic File
# Line 1 appearance
line1_name: 1234

# Line 1 Registration Authentication
line1_authname: 1234

# Line 1 Registration Password
line1_password: 1234

# Phone Label (Text desired to be displayed in upper right corner)
phone_label: 1234; Has no effect on SIP messaging

# Line 1 Display Name (Display name to use for SIP messaging)
line1_displayname: 1234

# Proxy Server
proxy1_address: 10.0.1.1
proxy2_address:""; Can be dotted IP or FQDN
proxy3_address:""; Can be dotted IP or FQDN
proxy4_address:""; Can be dotted IP or FQDN
proxy5_address:""; Can be dotted IP or FQDN
proxy6_address:""; Can be dotted IP or FQDN

# Proxy Server Port (default - 5060)
proxy1_port: 5060
proxy2_port: 5060
proxy3_port: 5060
proxy4_port: 5060
proxy5_port: 5060
proxy6_port: 5060

# Proxy Registration (0-disable (default), 1-enable)
proxy_register: 1

# Phone Registration Expiration [1-3932100 sec] (Default - 3600)
timer_register_expires: 3600

# Codec for media stream (g711ulaw (default), g711alaw, g729a)
preferred_codec: g711ulaw
```

```
# TOS bits in media stream [0-5] (Default - 5)
tos_media: 5

# Inband DTMF Settings (0-disable, 1-enable (default))
dtmf_inband: 1

# Out of band DTMF Settings
#(none-disable, avt-avt enable (default), avt_always-always avt)
dtmf_outofband: avt

# DTMF dB Level Settings
#(1-6dB down, 2-3db down, 3-nominal (default), 4-3db up, 5-6dB up)
dtmf_db_level: 3

# SIP Timers
timer_t1: 500; Default 500 msec
timer_t2: 4000; Default 4 sec
sip_retx: 10; Default 10
sip_invite_retx: 6; Default 6
timer_invite_expires: 180 ; Default 180 sec

# Dialplan template (.xml format file relative to the TFTP root directory)
dial_template: dialplan

# TFTP Phone Specific Configuration File Directory
tftp_cfg_dir: ""; Example: ./sip_phone/

# Time Server
#(There are multiple values and configurations refer to Admin Guide for
Specifics)
sntp_server: 10.0.1.1; SNTP Server IP Address
sntp_mode: anycast (default); unicast, multicast, or directedbroadcast
time_zone: EST; Time Zone Phone is in
dst_offset: 1; Offset from Phone's time when DST is in effect
dst_start_month: April; Month in which DST starts
dst_start_day: ""; Day of month in which DST starts
dst_start_day_of_week: Sun; Day of week in which DST starts
dst_start_week_of_month: 1; Week of month in which DST starts
dst_start_time: 02; Time of day in which DST starts
dst_stop_month: Oct; Month in which DST stops
dst_stop_day: ""; Day of month in which DST stops
dst_stop_day_of_week: Sunday; Day of week in which DST stops
dst_stop_week_of_month: 8; Week of month in which DST stops 8=last week of
month
dst_stop_time: 2; Time of day in which DST stops
```

```
dst_auto_adjust: 1; Enable(1-Default)/Disable(0) DST automatic adjustment
time_format_24hr: 1; Enable(1 - 24Hr Default)/Disable(0 - 12Hr)


# Do Not Disturb Control
#(0-off (default), 1-on, 2-off with no user control, 3-on with no user
control)
dnd_control: 0;


# Caller ID Blocking
#(0-disabled, 1-enabled, 2-disabled no user control, 3-enabled no user
control)
callerid_blocking: 0; (Default is 0 - disabled and sending all calls as
anonymous)


# Anonymous Call Blocking
#(0-disabled, 1-enabled, 2-disabled no user control, 3-enabled no user
control)
anonymous_call_block: 0; (Default is 0 - disabled and blocking of anonymous
calls)


# DTMF AVT Payload (Dynamic payload range for AVT tones - 96-127)
dtmf_avt_payload: 101; Default 101


# Sync value of the phone used for remote reset
sync: 1; Default 1


# Backup Proxy Support
proxy_backup: ""; Dotted IP of Backup Proxy
proxy_backup_port: 5060; Backup Proxy port (default is 5060)


# Emergency Proxy Support
proxy_emergency: ""; Dotted IP of Emergency Proxy
proxy_emergency_port: 5060; Emergency Proxy port (default is 5060)


# Configurable VAD option
enable_vad: 0; VAD setting 0-disable (Default), 1-enable


# NAT/Firewall Traversal
nat_enable: 0; 0-Disabled (default), 1-Enabled
nat_address: ""; WAN IP address of NAT box (dotted IP or DNS A record only)
voip_control_port: 5060; UDP port used for SIP messages (default - 5060)
start_media_port: 16384; Start RTP range for media (default - 16384)
end_media_port: 32766; End RTP range for media (default - 32766)
nat_received_processing: 0; 0-Disabled (default), 1-Enabled


# Outbound Proxy Support
outbound_proxy: ""; restricted to dotted IP or DNS A record only
```

```
outbound_proxy_port: 5060; default is 5060

# Allow for the bridge on a 3way call to join remaining parties upon hangup
cnf_join_enable: 1; 0-Disabled, 1-Enabled (default)

# Allow Transfer to be completed while target phone is still ringing
semi_attended_transfer: 1; 0-Disabled, 1-Enabled (default)

# Telnet Level (enable or disable the ability to Telnet into the phone)
telnet_level: 2; 0-Disabled (default), 1-Enabled, 2-Privileged

# XML URLs
services_url: ""; URL for external Phone Services
directory_url: ""; URL for external Directory location
logo_url: "http://httpserver.isp.com/usage/phone.bmp"; URL for branding
logo to be used on phone display

# HTTP Proxy Support
http_proxy_addr: ""; Address of HTTP Proxy server
http_proxy_port: 80; Port of HTTP Proxy Server (80-default)

# Dynamic DNS/TFTP Support
dyn_dns_addr_1: ""; restricted to dotted IP
dyn_dns_addr_2: ""; restricted to dotted IP
dyn_tftp_addr: ""; restricted to dotted IP

# Remote Party ID
remote_party_id: 0; 0-Disabled (default), 1-Enabled
```

Annex B-Call Admission Controller algorithm

The Session Controller (SC) uses the following Call Admission Controller (CAC) algorithm:

1. During the start process for a call, allocate sufficient bandwidth for a G.711 10 ms call.
2. **After negotiation of the CODEC type (SDP protocol), adjust the bandwidth allocation to the maximum bandwidth for the CODEC type.**
3. **When the RTP stream starts, adjust the bandwidth allocation based on the observed packet time.**

The following example assumes a SIP call over WAN Ethernet (with a 14-byte Ethernet header included in the calculations):

1. When an INVITE message is received to start a call, the SC allocates 107 200 bps (100 pps x 134 bytes x 8 bits), corresponding to a G.711 10ms CODEC.

2. **When the 200 OK is received (assuming use of the G.729a CODEC), the SC adjusts the bandwidth to 51 200 bps (100 pps x 64 bytes x 8 bits).**
3. **When the media is started (assuming the observed packet time is G.729a 20ms), the SC adjusts the bandwidth to 29 600 bps (50 pps x 74 bytes x 8 bits).**

To ensure use of all available bandwidth, the Session Controller makes an additional adjustment when the remaining bandwidth is insufficient for a G.711 10ms call. (The above CAC algorithm would reject the call in step 1) Instead, the G.711 CODEC, if present, is removed from the SDP body before the INVITE/SDP messages are relayed. (This prevents establishment of the call with that CODEC.) Instead, CAC allocates the maximum bandwidth that could be used by the remaining CODECs.

The limitations of this algorithm are:

- Endpoints must not change the payload type without renegotiating it through signaling.
- Because every call requires an initial reservation of the maximum possible bandwidth (107 200 bps), this limits the rate at which calls can be established. (The CAC must wait for the end of the SDP negotiation before it can adjust the bandwidth allocation.)

16
VoIP Services and Relays

This chapter describes services that the BSGX4e device can provide for the VoIP phones and other devices on its LAN.

Each user device on the LAN (such as IP phones and PCs) can be configured, either manually or through DHCP, to use the BSGX4e as its DNS, SNTP, and TFTP server. To perform these server functions, the BSGX4e intelligently relays requests from clients on the LAN to servers on the WAN. This makes it easier to provision and manage multiple user devices.

The following services are available:

- **DHCP server** and **DHCP relay** function to acquire IP addresses.
- **DNS relay** function to acquire domain resolutions. This function can be needed for HTTP URLs to display logos.
- **SNTP relay** function to provide synchronization with an SNTP server.
- **TFTP relay** function to acquire configuration information.
- **TFTP file caching** to acquire upgrades.

DHCP Server

The DHCP server can provide IP addresses to up to 500 users. Lease information is saved in nonvolatile memory, so this information can be retrieved immediately after a restart.

Default DHCP Server Configuration

The initial configuration of the BSGX4e device includes a DHCP server configured on its LAN interface (eth1). To see the initial configuration, enter the following command:

```
> show dhcps pool
DHCP Pools:
   Interface          eth1
   Subnet             192.168.1.0
   Netmask            255.255.255.0
   IP                 192.168.1.50 - 192.168.1.250
   Broadcast          192.168.1.255
   Lease              7 days

Options:
   Gateway           192.168.1.1
   DNS1              192.168.1.1
```

```
DNS2                0.0.0.0
TFTP
Filename
Domain
NTP1                  0.0.0.0
NTP2                  0.0.0.0
Timezone GMT Offset   0 [hh:mm]
150                   0.0.0.0
151                   0.0.0.0
160                   0.0.0.0
161                   0.0.0.0
```

DHCP Server Configuration Command

To change the DHCP server configuration, enter the following command:

```
> config dhcps pool
```

Table 91 describes the parameters for **config dhcps pool.**

Table 91. DHCP Server Configuration Parameters

Parameter	Description
[interface]	LAN interface on which the DHCP server provides IP addresses, either **eth1** or a virtual interface defined on eth1 (**vif***n*, where n=0-15).
subnet	Subnet (LAN interface IP address).
netmask	Netmask to use.
ip	IP address range to use for addresses in the pool.
broadcast	Broadcast address.
lease	Offered lease length in days (1—7).
gateway	Default router.
dns1	IP address of the primary DNS server.
dns2	IP address of the secondary DNS server.
tftp	IP address of the TFTP server.
filename	File name of the TFTP server to pass to client.
domain	Domain name to supply to clients.
ntp1	IP address of the primary SNTP server.
ntp2	IP address of the secondary SNTP server.
gmtoffset	Time zone offset from GMT ([+/-]hh:mm).
opt_150	Option 150 value (used by some models of Cisco phones).
opt_151	Option 151 value (used by some models of Cisco phones).
opt_160	Option 160 value (used by some models of Polycom phones).
opt_161	Option 161 value (used by some models of Polycom phones).

DHCP Server Configuration Example

This example configures the DHCP server, so it can provide DNS, TFTP, and SNTP relay services for the LAN devices. The IP address of the eth1 interface of the BSGX4e device is 10.0.1.1.

```
> config dhcps pool eth1
Entering interactive mode ctrl^z | 'exit', ctrl^c | 'quit'
*dhcps-pool-eth1#*>    subnet     10.0.1.0
*dhcps-pool-eth1#*>    netmask    255.255.255.0
*dhcps-pool-eth1#*>    ip         10.0.1.100 - 10.0.1.200
*dhcps-pool-eth1#*>    broadcast  10.0.1.255
*dhcps-pool-eth1#*>    lease      1
*dhcps-pool-eth1#*>    gateway    10.0.1.1
*dhcps-pool-eth1#*>    dns1       10.0.1.1
*dhcps-pool-eth1#*>    tftp       10.0.1.1
*dhcps-pool-eth1#*>    domain     lan.com
*dhcps-pool-eth1#*>    ntp1       10.0.1.1
*dhcps-pool-eth1#*>    gmtoffset     +9
*dhcps-pool-eth1#*>    opt_150    10.0.1.1
*dhcps-pool-eth1#*>    opt_151    10.0.1.1
*dhcps-pool-eth1#*>    opt_160    10.0.1.1
*dhcps-pool-eth1#*>    opt_161    10.0.1.1
*dhcps-pool-eth1#*>    exit

*> save
```

Show DHCP Server Configuration

To view the DHCP server configuration, enter the following command:

```
> show dhcps pool

DHCP Pools:
   Interface           eth1
   Subnet              10.0.1.0
   Netmask             255.255.255.0
   IP                  10.0.1.100 - 10.0.1.200
   Broadcast           10.0.1.255
   Lease               1 days

Options:
   Gateway             10.0.1.1
   DNS1                10.0.1.1
   DNS2                0.0.0.0
   TFTP                10.0.1.1
   Filename
   Domain              lan.com
   NTP1                10.0.1.1
   NTP2                0.0.0.0
   Timezone Offset     +9 [hh:mm]
   150                 10.0.1.1
```

```
151                 10.0.1.1
160                 10.0.1.1
161                 10.0.1.1
```

Show DHCP Leases

To view the DHCP leases, enter the following command:

```
> show dhcps lease
```

```
DHCP Leases:

IP              StartTime                 Hostname            Expired
                EndTime                   MAC
-------------------------------------------------------------------
192.168.1.55    2006/08/28 15:13:28       NA                  *
                2006/08/28 15:15:28       00:0f:8f:07:2d:3d
192.168.1.52    2006/08/28 14:48:44       hyeres              *
                2006/08/28 14:50:44       00:11:43:29:2d:ed
```

The **IP** field lists the IP address of the device that holds the lease.

The **Hostname** and **MAC** fields report the host name and MAC address of the leasee.

The **Expired** field shows an asterisk (*) if the current system time is greater than the end time of the lease. This indicates that the lease is expired.

DHCP Relay

The DHCP relay function relays DHCP messages between clients located on the LAN and a single server located on the WAN. From the viewpoint of the clients on the LAN, the BSGX4e appears to be the server. From the viewpoint of the server on the WAN, the BSGX4e appears to be the client.

NOTE: To use the DHCP relay, you must disable the DHCP client on the WAN interface, disable the DHCP server on the LAN interface, and disable NAT on the eth0 interface.

DHCP Relay Command

For DHCP relay, enter the following command:

```
> config relay dhcp settings
```

Table 92 describes the parameters for **config relay dhcp settings**.

Table 92. DHCP Relay Parameters

Parameters	Description
enabled	Indicates whether to enable DHCP relay (Boolean). The initial setting is **no** (disabled).

Table 92. DHCP Relay Parameters (continued)

Parameters	Description
server	DHCP server on the WAN to which LAN DHCP messages are relayed.

DHCP Relay Example

The following example enables the DHCP relay function and specifies the DHCP server at IP address 192.168.134.200:

```
> config relay dhcp settings enabled yes server
192.168.134.200
*> save
```

Show DHCP Relay Settings

To verify the configuration, enter the following command:

```
> show relay dhcp settings

DHCP Relay Settings:

   Enabled     yes
   Server      192.168.134.200
```

DNS Relay

The DNS relay function relays DNS messages between clients located on LAN and a single DNS server located on the WAN. It sets up the BSGX4e device as a proxy for clients on the LAN who must make DNS requests (such as those required for Web browsing, and e-mail). From the viewpoint of the clients on the LAN, the BSGX4e appears to be the server. From the viewpoint of the server on the WAN, the BSGX4e appears to be the client.

The BSGX4e maintains a cache filled with the successful DNS exchanges. If a DNS request is already in the cache, the BSGX4e can reply to the DNS request without referencing a DNS server.

NOTE: Configure devices on the LAN, either through DHCP (option 6) or manually, to use the BSGX4e as their DNS server.

DNS Relay Command

For the DNS relay function, enter the following command:

```
> config relay dns settings
```

Table 93 describes the parameters for **config relay dns settings**.

Table 93. DNS Relay Parameters

Parameters	Description
enabled	Indicates whether the DNS relay is enabled (Boolean). The initial setting is **no** (disabled).
dns1	IP address of the primary external DNS server.
dns2	IP address of an optional second external DNS server.
dhcp	Indicates whether the DNS server addresses are provided by the DHCP client on the WAN interface of the BSGX4e (on | off). The initial setting is **off**.

DNS Relay Example

The following example enables the DNS relay function and specifies the DNS server at IP address 192.168.134.201:

```
> config relay dns settings enabled yes dns1 192.168.134.201
*> save
```

Show DNS Relay Settings

To verify the configuration, enter the following command:

```
> show relay dns settings

DNS Relay Settings:

   Enabled     on
   DNS1        192.168.134.201
   DNS2        0.0.0.0
   DHCP        off
```

Show DNS Sessions

To show the current DNS sessions exchanged through the BSGX4e, enter the following command:

```
> show relay dns sessions

DNS Relay Sessions:

Index Client                    Request Id Duration
------------------------------------------------------------
1     10.0.2.51:3639            2          4
2     10.0.2.51:3640            3          2
3     10.0.2.51:3641            1          0
```

Show DNS Relay Cache

To show the contents of the DNS relay cache, enter the following command:

```
> show relay dns cache

DNS Relay Cache:

Index Name                  IP address            TTL
-------------------------------------------------------------
1     tftpserver.wan.com    192.168.134.161       56
```

SNTP Relay

The SNTP relay function relays the SNTP messages between clients located on the LAN and a single server located on the WAN. From the viewpoint of the clients on the LAN, the BSGX4e appears to be the server. From the viewpoint of the server on the WAN, the BSGX4e appears to be the client.

NOTE: Configure devices on the LAN, either through DHCP (option 42) or manually, to use the BSGX4e as their SNTP server.

SNTP Relay Command

For SNTP relay, enter the following command:

```
> config relay sntp settings
```

Table 94 describes the parameters for **config relay sntp settings**.

Table 94. SNTP Relay Configuration Parameters

Parameters	Description
enabled	Enables the SNTP relay function (Boolean) (**on** | **off**). The initial setting is **off**.
server	IP address or FQDN of the external SNTP server.
dhcp	Indicates whether the SNTP server address is provided by the DHCP client on the WAN interface of the BSGX4e (**on** | **off**). The initial setting is **off**.
gmt	GMT time zone offset in hours (+ or -). The default is **0**. Specify this offset only if the client devices cannot provide their offset. If the appropriate offset is supplied by the clients, set this parameter to **0**.

SNTP Relay Example

The following example enables the SNTP relay function and specifies the SNTP server at IP address 192.168.134.160. The **gmt** parameter is set to **0**, so the BSGX4e device does not provide the time offset.

```
> config relay sntp settings enabled yes server
192.168.134.160 gmt 0
*> save
```

Show SNTP Settings

To verify the SNTP settings, enter the following command:

```
> show relay sntp settings

SNTP Relay Settings:

   Enabled     on
   Server      192.168.134.160
   DHCP        off
   GMT         0 hours
```

Show SNTP Sessions

To show the current SNTP sessions exchanged through the BSGX4e, enter the following command:

```
> show relay sntp sessions

SNTP Relay Sessions:

Index Client                    Relay                  Duration
-------------------------------------------------------------
1     10.0.2.51:123              192.168.134.217:2001   4
```

TFTP Relay

TFTP relay function relays the TFTP messages between clients located on the LAN and a single server located on the WAN. From the viewpoint of the clients on the LAN, the BSGX4e appears to be the server. From the viewpoint of the server on the WAN, the BSGX4e appears to be the client.

The BSGX4e maintains a cache filled with the successful TFTP exchanges. If a TFTP request is already in the cache, the BSGX4e can reply to the TFTP request without referencing a TFTP server.

NOTE: Configure devices on the LAN, either through DHCP (option 66, for example) or manually, to use the BSGX4e as the TFTP server.

TFTP Relay Command

For TFTP relay, enter the following command:

```
> config relay tftp settings
```

Table 95 describes the parameters for **config relay tftp settings.**

Table 95. TFTP Relay Configuration Parameters

Parameter	Description
enabled	Enables the TFTP relay (Boolean). The initial setting is **off**.

Table 95. TFTP Relay Configuration Parameters (continued)

Parameter	Description
server	IP address or FQDN of external TFTP server.
dhcp	Indicates whether the TFTP server address is provided by the DHCP client on the WAN interface of the BSGX4e (on | off). The initial setting is **off**.
allow	Types of TFTP messages to relay (**get** | **all**). The default is **get**.
sessions	Maximum number of concurrent TFTP sessions. This ensures that the CPU is not monopolized by TFTP packet relays. The default is **50**.

TFTP Relay Settings Example

The following example enables the TFTP relay function and specifies the FQDN of the TFTP server as `tftpserver.wan.com`:

```
> config relay tftp settings enabled yes server
tftpserver.wan.com
*> save
```

Show TFTP Relay Settings

To verify the TFTP relay settings, enter the following command:

```
> show relay tftp settings

TFTP Relay Settings:

   Enabled      on
   Server       tftpserver.wan.com
   DHCP         off
   Allow        get
   Sessions     50
```

Show TFTP Sessions

To show the current TFTP sessions exchanged through the BSGX4e, enter the following command:

```
> show relay tftp sessions

TFTP Relay Sessions:

Index Client          Relay                Server               Duration
                                                                packets
-------------------------------------------------------------------------
1     10.0.2.51:3639  192.168.134.191:2001 192.168.134.161:3001 4
```

TFTP File Cache

The TFTP cache feature allows copies of frequently requested files to be temporarily stored on the BSGX4e. If a file requested by a LAN device is found in the cache, it can be immediately sent to the client.

File caching provides the following benefits:

- Avoids unnecessary WAN bandwidth usage for frequently requested files, especially if several user devices exist, such as VoIP phones
- Improves scalability of VoIP service from a service provider, by reducing load on the central file servers that are used for provisioning user devices

NOTE: The TFTP relay function must be enabled.

TFTP Cache Command

For a TFTP file cache, enter the following command:

```
> config relay tftp cache
```

Table 96 describes the parameters for **config relay tftp cache**.

Table 96. TFTP Cache Configuration Parameters

Parameters	Description
enabled	Enables TFTP file caching (Boolean).The initial setting is **off**.
size	Size of the file cache in MegaBytes (MB) (**1**-**16**). The default is **6** MB.
refresh	Cache refresh interval (in minutes). The default is **240** minutes (4 hours).
download	Method for downloading files into the cache: **auto** Files are saved to the cache while being downloaded by the TFTP relay function. **tftp** Files are downloaded into the cache using an internal TFTP client. **ftp** Files are downloaded into the cache using an internal FTP client. The default is **auto**.
server	IP address or FQDN of the TFTP or FTP server.
user	User name if downloading files by FTP.
password	Password if downloading files by FTP.

Specifying Files to be Cached

To store a file in the TFTP file cache, you must specify the following command:

```
> config relay tftp files
```

NOTE: Only files that are specified by this command are cached.

Table 97 describes the parameters for **config relay tftp files**.

Table 97. TFTP Files Configuration Parameters

Parameters	Description
[index]	File index.
name	Name of file for caching.

TFTP Cache Example

The following example configures the TFTP cache:

Size of the cache: 16 MB
Refresh interval: 960 minutes (16 hours)
Download mode: auto
Files cached: SIPDefault.cnf

```
> config relay tftp cache enabled yes size 16 refresh 960
download auto
*> config relay tftp files 1 name SIPDefault.cnf*
*> save
```

Show TFTP Cache Settings and Usage

To see the TFTP cache settings and usage, enter the following command:

```
> show relay tftp cache

TFTP Relay Settings:

   Enabled      on
   Size         16 MB
   Usage        0 bytes (0 %)
   Refresh      960 min
   Download     auto
   Server
   User
   Password
```

Show TFTP Cache Contents

To verify the content of the TFTP file cache, enter the following command:

```
> show relay tftp files

Index Name                    Size      Downloaded TTL        Sessions
-------------------------------------------------------------------
1     SIPDefault.cnf          0         no         0          0
```

Delete Files to be Cached

To delete an entry from the list of files to be cached, specify the entry index on the command **del relay tftp files**.

For example, the following command deletes the entry for index 1:

```
> del relay tftp files 1
```

Clear TFTP Cache

To clear the TFTP file cache of its contents, enter the following command:

```
> clear relay tftp cache
```

After the cache is cleared, new copies of the files are downloaded.

17 MONITORING

This chapter describes the information that the BSGX4e device collects so that the system can be monitored.

The BSGX4e device provides the following monitoring information:

- Information displays
  - System exceptions
  - System hardware
  - System status
  - System operations summary
- System logs: audit logging and module logging
- Port statistics
- IP stack statistics

Show System Exceptions

If a system error occurs, an exception is triggered and saved in nonvolatile memory. The exception information can be useful to determine the system problem. To see the exception information, enter the following command:

```
> show system exceptions
```

When a system error occurs, information similar to the following is displayed:

```
Type                TLB load exception
Task                GWEBS
Time                THU NOV 24 07:13:49 2005
Vector              2
Program Counter     0x803D5148
Access Address      0x00000004
Status Register     0x3000FF01
Cause Register      0x00000008
```

Table 98 describes the fields in the display.

Table 98. System Exception Information Fields

Field	Description
Type	Type of the exception.
Task	Task during which the exception occurred.

Table 98. System Exception Information Fields (continued)

Field	Description
Time	Time at which the exception occurred.
Vector	Exception vector.
Program Counter	Exception program counter.
Access Address	Address accessed to cause exception.
Status Register	Exception status register.
Cause Register	Exception cause register.

Show Hardware Information

When reporting a problem, it is important to provide both system information (**show system info**) and hardware information about the unit. To see the hardware information, enter the following command:

```
> show system hardware

System Hardware Info:
Board      Rev ID  Description                              Chip
-------------------------------------------------------------------
DTVC       1   4   Mainboard                                Fusiv-200
TEL        1   7   1 FXS + 1 FXO                            SiLabs
SWITCH     1   7   LAN Ethernet Switch - 4                  Marvell
WAN        1   5   WAN Ethernet (100BaseT)                  Marvell
```

Show System Status

The system status information display includes the following:

- Software information
  - Boot code version
  - Application version
  - Time since last reboot
- Hardware information
  - System type
  - Memory size
  - MAC addresses of device interfaces
  - Serial number

To show system information, enter the following command:

```
> show system info

System Info:

   Unit Name       MyUnit
```

```
Bootcode Ver    1.10.00010
App. Ver        BSG T2 2.02.0138
System Type     BSGX4e
Memory          89/128 MB
MAC 0           00:22:11:44:33:04
MAC 1           00:22:11:44:33:05
Serial
Country         United States of America (US)
Temp            Unsupported
Up time         0y 0d 4h 33m 20s
```

Show System Operation Summary

To see a summary of BSGX4e operations, enter the following command:

```
> summary

System Summary:

System:

   Application:     BSG Series 2.00.1002
   Boot:            1.10.0012
   Model:           BSGX4e
   Uptime:          0 y 0d 1h 42m 23s
   Date:            THU AUG 31 16:47:33 2006
   CPU Busy:        25%
   Memory Usage:    81/128 MB

SIP:                              MGCP:

   Server:       SER            Server:        Not configured
   Status:       Connected       Status:        Survivability

Calls:                                 Calls:

   Active:          221                  Active:          0
   Succeeded:       1989                 Succeeded:       0
   Failed:          0                    Failed:          0
   No Bandwidth:    0                    No Bandwidth:    0

   Avg. MOS:        4.0

Data:

   Routing:         10930 PPS
   Forwarded:       3087931066
   DHCP Leases:     2
   DHCP Interface:  eth1
```

```
   IDS Attacks:     4340719
   NAT:             Enabled

Interfaces:

   eth0              2.3.4.5         (NAT)
   eth1              0.0.0.0
   vif0              10.1.1.1
   vif1              192.168.134.192
   vpn0              100.100.100.191
```

- The Avg. MOS statistic is calculated based on the MOS of the last 30 calls.
- Data statistics include:

Routing	Current load of the system—the number of packets routed per second.
Forwarded	Cumulative number of packets routed through the IP stack.
DHCP Leases	Number of IP addresses assigned by the DHCP server to LAN devices.
IDS attacks	Number of attacks detected by IDS.

Audit Logging

Audit logging logs events that affect system security, including system configuration changes and invalid logon attempts.

Audit logging fills a table of 100 entries in FIFO order.

NOTE: In the initial configuration, audit logging is enabled.

NOTE: In the current version, the audit log is not saved in nonvolatile memory; it cannot be retrieved after the unit restarts. However, module logging can save to a file (see "Module Logging" (page 325)).

Audit Log Command

Audit logging is initially enabled. To disable audit logging, enter the following commands:

```
> config audit status enabled no
*> save
```

To reenable audit logging, enter the following commands:

```
> config audit status enabled yes
*> save
```

Show Audit Log Status

To see the status of audit logging, enter the following command:

```
> show audit status
```

```
Audit Log:

   Enabled     no
```

Show Audit Log Entries

To see the entries currently in the audit log, enter the following command:

```
> show audit log

Audit log:

Message
------------------------------------------------------------
16:16:02: root CONFIG switch qos setting
16:16:02: root CONFIG interface ip eth0
```

The following examples show entries for two configuration changes. Entries for configuration changes use the following format:

- Timestamp
- User identifier
- Type of change

CONFIG	Setting change
DEL	Record deletion
CLEAR	Deletion of entire table.

- Feature changed

Clear Audit Log

To clear the audit log of all entries, enter the following command:

```
> clear audit log
```

Module Logging

The BSGX4e device supports both local module logging and remote module logging (udplog and syslog). Local module logging writes entries to an internal buffer; to view the log entries, use the command **show logging internal**.

NOTE: Initially, local module logging is enabled, but remote module logging is disabled.

You can configure message logging for specific system modules using:

- Message severity (levels 0-8). The most severe level is *emergency* (level **0)**.
- Message destination. The possible destinations are:
  - Internal buffer
  - Internal file (retrievable after a restart)

- Console
- UDP server
- Syslog server

Table 99 lists the severity and default destination of each message level.

Table 99. Message Severity

Severity Level	Message Level	Description	Default Destination
0	`emerg`	Emergency operation error.	Internal buffer.
1	`alert`	Alert level operation error.	Internal buffer.
2	`crit`	Critical operation error.	Internal buffer.
3	`error`	Low-level operation error.	Internal buffer.
4	`warn`	Warnings, such as a system attack.	Internal buffer.
5	`notice`	Notices.	Internal buffer.
6	`inform`	Informative messages.	Internal buffer.
7	`debug`	Debug messages, such as receipt of a SIP signaling packet.	Not logged.
8	`trace`	Trace messages.	Not logged.

Logging Level Command

You can be include or exclude specific message levels for a system module. To specify the message levels to be logged for a module, enter the following command:

```
> config logging modules
```

CAUTION: Modification of the default configuration can severely affect system performance.

Table 100 describes the parameters for **`config logging modules.`**

Table 100. Logging Modules Configuration Parameters

Parameter	Description
`[module]`	Name of the system module for which the logging level is specified.
`map`	Message levels to be included or excluded (**emergency** | **alert** | **critical** | **error** | **warning** | **notice** | **inform** | **debug** | **trace**). To include a level, use a plus (**+**) prefix; to exclude a level, use a minus (**-**) prefix.

Logging Level Example

The following example specifies that `debug` and `trace` messages *are* to be logged, and `inform` messages are *not* to be logged for module VQM:

```
> config logging modules VQM map +debug +trace
*> config logging modules VQM map -inform
*> save
```

Show Logging Levels

To show the logging level for system modules, enter the **show logging modules** command. To show the logging level for a specific module, specify the module on the command.

For example, the following command shows the logging level for module VQM:

```
> show logging modules VQM
```

```
Logging Levels:
Module Name Mapping Matrix
--------------------------------------------------------------------------------
VQM         emergency + alert + critical + error + warning + notice + debug
+trace
```

Mapping Log Destinations

Each type of log message is mapped to its own set of destinations. It can be sent to **all** destinations, to no destination (**none**), or to one or more specific destinations.

The possible log destinations are:

- **console:** Messages are displayed on the RS-232 console.
- **internal:** Messages are stored in an internal buffer of limited size, filled in FIFO order, but irretrievable after the unit restarts. The messages are displayed by the **`show logging internal`** command.
- **file:** Messages are stored in an internal file of limited size, filled in a FIFO order, and retrievable after the unit restarts. The messages are displayed by the **`show logging file`** command.

  Note: The file does not appear in the file system. It cannot be uploaded to a remote device.
- **UDP:** Messages are sent in raw UDP format to the UDP server specified by the **config logging destination** command.
- **syslog:** Messages are sent in Syslog format to the Syslog server specified by the **config logging destination** command.

Logging Map Command

To map each log message type to its own set of destinations, enter the following command:

```
> config logging map
```

Table 101 describes the parameters for **`config logging map`**.

NOTE: To include a specific destination in the map for a message type, use a plus (+) prefix; to exclude a destination, use a minus (-) prefix.

Table 101. Log Destination Map Parameters

Parameter	Description
emerg	Destinations for *Emergency* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **internal**.
alert	Destinations for *Alert* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **internal**.
crit	Destinations for *Critical* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **internal**.
error	Destinations for *Error* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **internal**.
warn	Destinations for *Warning* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **internal**.
notice	Destinations for *Notice* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **internal**.
inform	Destinations for *Inform* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **internal**.
debug	Destinations for *Debug* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **none**.
trace	Destinations for *Trace* messages (**all** | **console** + **udp** + **syslog** + **internal** + **file** | **none**). The default is **none**.

Log Destination Map Examples

The following command sends *Emergency* messages to the Syslog server:

```
> config logging map emerg +syslog
```

The following command stops the sending of *Inform* messages to the internal buffer:

```
*> config logging map inform -internal
*> save
```

Show Log Destination Map

To show the map of log message types and destinations, enter the following command:

```
> show logging map

Redirection Map:

   Emergency Map     syslog + internal
```

```
Alert Map          internal
Critical Map       internal
Error Map          internal
Warning Map        internal
Notice Map         internal
Inform Map
Debug Map
Trace Map
```

Show Module Log Entries

If one of the logging destinations for a message is **internal** (for internal buffer) or **file** (for an internal file retrievable after a restart), you can display the messages by using a command.

Messages stored in the internal buffer are displayed by the following command:

```
> show logging internal
```

Messages stored in an internal file (retrievable after a restart) are displayed by the following command:

```
> show logging file
```

Both commands show messages such as the following:

```
(W)16:44:16: Firewall denied [Id:0] [Src:192.168.134.71:137]
[Dst:192.168.134.255:137] [Proto:UDP] [If: 0]
(W)16:44:17: Firewall denied [Id:0] [Src:192.168.134.71:137]
[Dst:192.168.134.255:137] [Proto:UDP] [If: 0]
```

Each log message has the following format:

- Severity level, such as `(W)` for warning.
- Timestamp
- Message

Configure Log Server

If the destination map for a message type includes a server, the server must be configured. The server destinations are:

- **UDP:** Messages are sent in raw UDP format to the UDP server specified by the **config logging destination** command.
- **syslog:** Messages are sent in Syslog format to the Syslog server specified by the **config logging destination** command.

Log Server Configuration Command

Table 102 describes the configuration parameters for **`config logging destination`**.

Table 102. Log Server Parameters

Destination	Description
udpip	(For a **UDP** destination) IP address of a standard UDP receiver.
udpport	(For a **UDP** destination) Port of the receiving UDP logger.
sysip	(For a **Syslog** destination) IP address of a receiving Syslog daemon.
sysport	(For a **Syslog** destination) Port of a receiving Syslog daemon.
facility	(For a **Syslog** destination) Syslog facility to use (**local***n*, where *n* is 0-7).

Log Server Configuration Examples

The following example configures a UDP server:

Server: 192.168.22.60
Port: 1234

```
> config logging destination udpip 192.168.22.60 udpport 1234
*> save
```

The following example configures a Syslog server:

Server: 192.168.134.161
Port: 514
Facility: local0

```
> config logging destination sysip 192.168.134.161 sysport
514 facility local0
*> save
```

Show Log Server Configuration and Statistics

To show the configuration and statistics of the log servers, enter the following command:

```
> show logging destination

Config Info:

   UDP Logger IP       192.168.22.60
   UDP Logger Port     1234
   Syslog IP           192.168.134.161
   Syslog Port         514
   Syslog Facility     local0

Counters Info:

   MsgQTxErrors        0
   MsgQRxErrors        0
   LogTxCount          96
```

```
LogRxCount          96
Errors              0
```

Ethernet Interface Statistics

The BSGX4e device records layer 1 and layer 2 Ethernet statistics for its Ethernet interfaces.

To show the statistics for an Ethernet interface, specify the interface on the **stats interface ip** command.

For example, to see the statistics for *eth0*, enter the following command:

```
> stats interface ip eth0
eth0 Stats

Tx                1501208        Rx                1508267
OutUnicasts       1501197        In Unicasts       1507394
OutBroadcasts          11         InBroadcasts         720
OutPause                0         InPause              0
OutMulticasts           0         InMulticasts       153
OutFCSErr               0         InFCSErr             0
Out64Octets            83         In 64 Octets       795
Out127Octets      1499933        In127Octets       1506446
Out255Octets          574         In255Octets         68
Out511Octets          316         In511Octets        334
Out1023Octets         302         In1023Octets       624
OutMaxOctets            0         InMaxOctets          0
Deferred                0         InDiscards           0
Out Octets      117491330         InGoodOctets
118436014
AlignErr                0         InBadOctets          0
Oversize                0         Undersize            0
Jabber                  0         Fragments            0
Collisions              0         Late Collisions      0
Excessive               0         Filtered             0
Single                  0         Multiple             0
```

Clear Statistics

The following command clears the statistics kept for the eth0 interface:

```
> clear interface ip eth0
```

IP Stack Statistics

Layer 3 (IP) and layer 4 (ICMP, UDP, and TCP) statistics are provided for the IP routing stack.

IP Statistics

IP statistics report counters about the traffic routed through the IP stack. To see the IP statistics, use the following command:

```
> show protocol ip

IP Stats:

Bad Checksum            0               Total packets          1802
Packets Forwarded       0               Fragments Received     0
Too Small               0               Too Short              0
Bad Length              0               Bad Hlen               0
Frag Timeout            0               Frag Dropped           0
Cannot Forward          0               Fast Forward           0
No Proto                1               Redirect Sent          0
Local Out             722               Delivered           1135
Reassembled             0                Odropped              0
Output Fragments        0                Fragmented            0
Bad options             0                Cannot Fragment       0
Bad Version             0                No Route              0
Too Long                0                Raw Out               0
                                         Not Member            0
```

Table 103 describes the IP statistics.

Table 103. IP Statistics

Counter	Description
Bad Checksum	Bad checksum.
Total packets	Total packets.
Packets Forwarded	Packets forwarded.
Fragments Received	Fragments received.
Too Small	Fragments that have incoherent offset.
Too Short	Packet is less than minimum IP length.
Bad Length	IP length less than IP header length.
Bad Hlen	IP header length less than data size.
Frag Timeout	Fragments timed out.
Frag Dropped	Fragments dropped.
Fast Forward	Packets fast forwarded.
Cannot Forward	Packets received for an unreachable destination.
No Proto	Unknown or unsupported protocol.
Redirect Sent	Packets forwarded on the same network.
Local Out	Total number of IP packets generated.
Delivered	Datagrams delivered to upper level.
Reassembled	Total number of packets reassembled OK.

Table 103. IP Statistics (continued)

Counter	Description
Odropped	Lost packets due to no buffers.
Output fragments	Output fragments created.
Fragmented	Datagrams successfully fragmented.
Bad options	Error in options processing.
Cannot Fragment	*Do not fragment* flag is set.
Bad Version	IP version not equal to 4.
No Route	Packets discarded due to no route.
Too Long	IP length is greater than maximum IP packet size.
Raw Out	Total raw IP packets generated.
Not Member	Multicasts received for unregistered groups.

ICMP Statistics

ICMP statistics report counters about ICMP traffic that terminates at the IP stack. To see the ICMP statistics, use the following command:

```
> show protocol icmp

ICMP Stats:

Echo Reply Out          0               Echo Reply In          0
Dest Unrch Out          0               Dest Unrch In          2
Src Quench Out          0               Src Quench In          0
Redirect Out            0               Redirect In            0
Echo Out                0               Echo In                0
Time Exceed Out         0               Time Exceed In         0
Param Prob Out          0               Param Prob In          0
Timestamp Out           0               Timestamp In           0
Timestamp Reply Out     0               Timestamp Reply In     0
Info Req Out            0               Info Req In            0
Info Reply Out          0               Info Reply In          0
Mask Request Out        0               Mask Request In        0
Mask Reply Out          0               Mask Reply In          0
Old ICMP                0               Old Short              0
Too Short               0               Bad Code               0
Bad Length              0               Checksum               0
BMCast Echo Drop        0               Reflect                0
Errors                  0               BMCast TS Drop         0
```

Table 104 describes the ICMP statistics.

Table 104. ICMP Statistics

Counter	Description
Echo Reply Out	ICMP Echo Reply messages (ICMP: Msg 0).
Echo Reply In	ICMP Echo Reply messages (ICMP: Msg 0).
Dest Unrch Out	ICMP Destination Unreachable messages (ICMP: Msg 3).
Dest Unrch In	ICMP Destination Unreachable messages (ICMP: Msg 3).
Src Quench Out	ICMP Source Quench messages (ICMP: Msg 4).
Src Quench In	ICMP Source Quench messages (ICMP: Msg 4).
Redirect Out	IICMP Redirect messages (ICMP: Msg 5).
Redirect In	ICMP Redirect messages (ICMP: Msg 5).
Echo Out	ICMP Echo messages (ICMP: Msg 8).
Echo In	ICMP Echo messages (ICMP: Msg 8).
Time Exceed Out	ICMP Time Exceeded messages (ICMP: Msg 11).
Time Exceed In	ICMP Time Exceeded messages (ICMP: Msg 11).
Param Prob Out	ICMP Parameter Problems messages (ICMP: Msg 12).
Param Prob In	ICMP Parameter Problems messages (ICMP: Msg 12).
Timestamp Out	ICMP Timestamp messages (ICMP: Msg 13).
Timestamp In	ICMP Timestamp messages (ICMP: Msg 13).
Timestamp Reply Out	ICMP Timestamp Reply messages (ICMP: Msg 14).
Timestamp Reply In	ICMP Timestamp Reply messages (ICMP: Msg 14).
Info Req Out	ICMP Information Request messages (ICMP: Msg 15).
Info Req In	ICMP Information Request messages (ICMP: Msg 15).
Info Reply Out	ICMP Info Reply messages (ICMP: Msg 16).
Info Reply In	ICMP Info Reply messages (ICMP: Msg 16).
Mask Request Out	Mask Request Out.
Mask Request In	Mask Request In.
Mask Reply Out	Mask Reply Out.
Mask Reply In	Mask Reply In.
Old ICMP	Problem since old packet was ICMP.
Old Short	Old IP packet is too short.
Too Short	Packet is less than minimum ICMP length.
Bad Code	ICMP code is out of range or unsupported.
Bad Length	Bad length due to bounds calculation.
Checksum	Bad checksum detected on packet.
BMcast Echo Drop	Broadcast /multicast echo requests dropped.

Table 104. ICMP Statistics (continued)

Counter	Description
Reflect	Number of responses.
Errors	ICMP had a problem dealing with the packet.
BMcast Time Drop	Broadcast / multicast timestamp requests dropped.

UDP Statistics

UDP statistics report counters about UDP traffic that terminates at the IP stack. To see the UDP statistics, enter:

```
> show protocol udp

UDP Stats:

Out                 176                  In                  196
Header Drops          0                   Out Fastpath         0
Bad Length            0                   Bad ChkSum           0
No Port (BCast)       0                   No Port              0
PCB Cache Miss        0                   Full Socket          0
                                          PCB Hash Miss        0
```

Table 105 describes the UDP statistics.

Table 105. UDP Statistics

Counter	Description
Out	Total packets out.
In	Total packets in.
Header Drops	Packet length shorter than header length.
Out Fastpath	Packet output on hardware fastpath.
Bad Length	Data length greater than packet length.
Bad ChkSum	Bad checksum error on packet.
No Port (BCast)	No socket listening on port (Broadcast).
No Port	No socket listening on port.
PCB Cache Miss	Protocol Control Block cache misses.
Full Socket	Number of times that the socket is too full to deliver packet.
PCB Hash Miss	Protocol Control Block hash misses.

TCP Statistics

TCP statistics report counters about TCP traffic that terminates at the IP stack. To see the TCP statistics, use the following command:

```
> show protocol tcp
```

```
TCP Stats:

Connections Accepted      1       Connections Attempted     0
Connections Dropped       0       Connections Established   1
Connections Closed        2       Emb Conn Dropped          0
RTT Updated               600     Segments Timed            600
Timeout Drop              0       Delayed Acks              35
Persistent Timeouts       0       Retransmit Timeouts       0
Keepalive Probes          0       Keepalive Timeouts        0
Total Sent                635     Keepalive Drops           0
Bytes Sent                44888   Packets Sent              599
Bytes Retransmitted       0       Packets Retransmitted     0
Probes Sent               0       Acks Sent                 36
Window Update Sent        0       Urgent Sent               0
Total Received            1091    Control Sent              0
Bytes Received            874     Packets Received          536
Offset Error              0       Checksum Error            0
Duplicate Packets         0       Too Short                 0
Part Duplicate Packets    0       Duplicate Bytes           0
Out-of-order Packets      0       Part Duplicate Bytes      0
After Window Packets      0       Out-of-order Bytes        0
After Close Packets       0       After Window Bytes        0
Dup Ack Packets           0       Window Probe Packets      0
Ack Packets               600     Unsent Data Ack Packets   0
Window Update             0       Ack Bytes                 44889
Predicate ack             543     PAWS Dropped              0
Cache Missed              0       Predicate data            490
Cached RTT Var            0       Cached RTT                0
Used RTT                  0       Cached SSThresh           0
Used SS Thresh            0       Used RTT Var              0
Bad SYN                   0       Persistent Drop           0
```

Table 106 describes the TCP statistics.

Table 106. TCP Statistics

Counter	Description
Connections Accepted	Total connections accepted.
Connections Attempted	Total connections initiated.
Connections Dropped	Connections dropped.
Connections Established	Total connections established.
Connections Closed	Connections closed (includes dropped).
Emb Conn Dropped	Embryonic connections dropped.
RTT Updated	RTT updated.
Segments Timed	Segments where RTT was determined.

Table 106. TCP Statistics (continued)

Counter	Description
Timeout Drop	Connections dropped in retransmit timeout.
Delayed Acks	Delayed acks sent.
Persistent Timeouts	Persistent timeouts.
Retransmit Timeouts	Retransmit timeouts.
Keepalive Probes	Keepalive probes sent.
Keepalive Timeouts	Keepalive timeouts.
Total Sent	Total packets sent.
Keepalive Drops	Connections dropped in keepalive.
Bytes Sent	Data bytes sent.
Packets Sent	Data packets sent.
Bytes Retransmitted	Data bytes retransmitted.
Packets Retransmitted	Data packets retransmitted.
Probes Sent	Probe packets sent.
Acks Sent	Ack-only packets sent.
Window Update Sent	Window update packets sent.
Urgent Sent	Urgent packets sent.
Total Received	Total packets received.
Control Sent	Control packets sent.
Bytes Received	Total bytes received in sequence.
Packets Received	Total packets received in sequence.
Offset Error	Total packets received with bad offset.
Checksum Error	Total packets received with checksum error.
Duplicate Packets	Total duplicate-only packets received.
Too Short	Total packets received too short.
Part Duplicate Packets	Total packets with some duplicate data.
Duplicate Bytes	Total duplicate-only bytes received.
Out-of-order Packets	Total out-of-order packets received.
Part Duplicate Bytes	Duplicate bytes in partial-duplicate packets.
After Window Packets	Total after window packets received.
Out-of-order Bytes	Total out-of-order bytes received.
After Close Packets	Total after close packets received.
After Window Bytes	Total after window bytes received.
Dup Ack Packets	Total duplicate ack packets received.
Window Probe Packets	Total window probe packets received.
Ack Packets	Total ack packets received.

Table 106. TCP Statistics (continued)

Counter	Description
Unsent Data Ack Packets	Total ack packets received for unsent data.
Window Update	Total window update packets received.
Ack Bytes	Total ack bytes.
Predicate ack	Total times header predicate OK for acks.
PAWS Dropped	Total segments dropped due to Protect Against Wrapped Segments (PAWS).
Cache Missed	Total times cache missed.
Predicate Data	Total times header predicate OK for data packets.
Cached RTT Var	Total times cached RTTVAR updated.
Cached RTT	Total times cached RTT in route updated.
Used RTT	Total times RTT initialized from route.
Cached SSThresh	Total times cached SSThresh updated.
Used SS Thresh	Total times Slow-Start (SS) Thresh initialized from route.
Used RTT Var	Total times RTT Var initialized from route.
Bad SYN	Bogus SYN (for example, premature ACK).
Persistent Drop	Timeout in persistent state.

18 MONITORING TOOLS

This chapter describes the tools provided for monitoring the operations of the BSGX4e device.

The BSGX4e device supports the following monitoring tools:

- Port mirroring
- Protocol monitoring (PMON) tool
- Netflow exporter
- SNMP agent
- TCPdump command
- Ping and traceroute commands

Port Mirroring

Port mirroring duplicates traffic from one or several source ports to a destination port.

The following port traffic can be mirrored:

- outgoing traffic only
- both incoming and outgoing traffic

NOTE: Port mirroring is intended for troubleshooting only. After its use is complete, remove the port mirroring configuration immediately so that unit performance is not degraded.

Port Mirroring Constraints

The following constraints apply to port mirroring:

- Port mirroring applies only to LAN ports.
- The mirroring port and the port being mirrored must have the same speed.
- The device cannot mirror incoming traffic only.
- No physical indicator exists to show that a port is set up for mirroring.

Port Mirroring Command

To set up port mirroring, enter the following command:

```
> config switch mirror
```

Table 107 describes the parameters for **`config switch mirror`**.

Table 107. Mirroring Parameters

Parameter	Description
[port]	Port for which traffic is mirrored (1 - 4).
mirror	Destination port where the mirrored traffic is sent (1 - 4). If mirroring is currently occurring, the default is the current destination port.
dir	Direction of traffic to mirror (**both** | **out** | **none**). The default is **both**. Specify **none** to suspend mirroring.

Mirroring Configuration Example

This example configures mirroring so that **both** incoming and outgoing traffic for port **2** is mirrored to port **3**:

```
> config switch mirror 2 mirror 3
*> save
```

Show Mirroring Configuration

To show the port mirroring configuration, enter the following command:

```
> show switch mirror

Switch Mirror:
Port  To   Direction
-------------------------------------------------------------
0-2   3    Both
```

Deleting a Port Mirroring Entry

To remove a mirroring entry and end mirroring for that port, enter the port number on the **del switch mirror** command.

For example, to remove the mirroring entry for port 2, use the following commands:

```
> del switch mirror 2
*> save
```

Protocol Monitoring (PMON)

The Protocol Monitoring (PMON) tool monitors traffic coming into the BSGX4e unit. PMON can record one or more traces of the incoming traffic.

NOTE: Only incoming traffic is monitored.

The following statistics are reported by each trace:

- Number of packets (received)
- Number of bytes (received)

- Packet rate
- Bit rate

PMON creates traces by applying filters to the traffic received on the WAN interface. The filters can apply to:

- Port (source or destination)
- IP address (source or destination)
- IP ToS tag value
- VLAN ID
- IP protocol
- MAC address (source or destination)
- Interface

When more than one filter is specified, a logical AND is applied.

PMON records statistics in five-minute intervals over a 24-hour period, thus recording 288 intervals. After 24 hours, PMON wraps statistics in FIFO (first-in first-out) order.

All monitoring traces are synchronized. This allows easy comparison of the traffic types received over a given period of time.

To use the PMON tool:

1. Enable the PMON agent.
2. Configure at least one trace.
3. Later, display the trace statistics.
4. Disable the PMON agent when monitoring is complete.

Enable PMON Command

To enable the PMON tool, enter the following command:

```
> config pmon agent enabled
```

When protocol monitoring is complete, disable the PMON tool with the following command:

```
> config pmon agent enabled no
```

PMON Trace Command

To configure a PMON trace, enter the following command:

```
> config pmon trace
```

Table 108 describes the parameters for **config pmon trace**.

Table 108. PMON Trace Parameters

Parameter	Description
[TraceName]	Name of the trace to add or change.
sourceport	Source port to monitor.
destport	Destination port to monitor.
srcip	Source IP address to monitor.
dstip	Destination IP address to monitor.
tos	ToS tag value to monitor.
vlanid	VLAN ID value to monitor.
ipproto	IP protocol to monitor (**any** | **udp** | **tcp** | **icmp**). The default is **any**.
srcmac	Source MAC address to monitor.
dstmac	Destination MAC address to monitor.
interface	Interface to monitor.

PMON Configuration Example

The following example starts the PMON agent and then configures a PMON trace named *VoIP*. The trace monitors traffic coming from IP address 10.0.1.100 and tagged with IP ToS tag value 248:

```
> config pmon agent enable yes
*> config pmon trace VoIP srcip 10.0.1.100 tos 248
*> save
```

Show PMON Status

To show the status of the PMON agent, enter the following command:

```
> show pmon agent

Status:

   Enabled     yes
```

Show PMON Traces

To show the PMON trace configuration, enter the following command:

```
> show pmon trace

PMON Trace:

   Trace           VoIP
   Source Port     10.0.1.100
   Dest Port       ANY
```

```
Source IP       ANY
Dest IP         ANY
ToS             248
Vlanid          ANY
IP Proto        ANY
Source MAC      ANY
Dest MAC        ANY
Interface       ANY
```

Show PMON Trace Statistics

To see the statistics recorded by a PMON trace, specify the trace name on a **stats pmon trace** command.

For example, the following command displays the statistics for the *VoIP* trace:

```
> stats pmon trace VoIP

PMON Stats:

Trace      Time Packets Byte Count   Packets Per Second Bits Per Second
-------------------------------------------------------------------------
VoIP       0    0       0            0                  0
VoIP       1    0       0            0                  0
VoIP       2    0       0            0                  0
VoIP       3    0       0            0                  0
VoIP       4    0       0            0                  0
```

The `Time` field reports the number of the time interval (from 0 to 287).

Clear PMON Trace Statistics

To clear the statistics recorded for the PMON trace VoIP, enter the following command:

```
> clear pmon trace VoIP
```

To clear the statistics recorded for all PMON traces, enter the following command:

```
> clear pmon trace all
```

Netflow Exporter

The BSGX4e unit implements a Netflow exporter. It monitors traffic coming into the unit and reports it to the Netflow collector. Netflow versions 1, 5, and 9 are supported.

NOTE: You must deploy the Netflow exporter with a Netflow collector. The exporter and collector must implement the same Netflow version.

NOTE: Only incoming traffic is monitored.

To classify traffic into the flow to be monitored, the Netflow exporter applies filters to the traffic received on the WAN interface. The filters can apply to:

- Port (source or destination)
- IP address (source or destination)
- IP ToS tag value
- IP protocol
- Ethernet protocol
- MAC address (source or destination)
- Interface

When more than one filter is specified, a logical AND is applied.

For the monitored traffic flow, the Netflow exporter reports the following information to the Netflow collector:

- Source IP address (IPV4_SRC_ADDR)
- Destination IP address (IPV4_DST_ADDR)
- Protocol (PROTOCOL)
- Source port (L4_SRC_PORT)
- Destination port (L4_DST_PORT)
- Number of packets received (IN_PKTS)
- Number of bytes received (IN_BYTES)
- Time since flow creation (FIRST_SWITCHED)
- Time since last update (LAST_SWITCHED)

To use the Netflow exporter:

1. Enable and configure the Netflow exporter, specifying the Netflow collector.
2. Configure filters to determine the traffic flow to be monitored.
3. Disable the Netflow exporter when monitoring is complete.

Netflow Exporter Command

To configure the Netflow exporter, enter the following command:

```
> config netflow agent
```

Table 109 describes the parameters for **config netflow agent.**

Table 109. Netflow Agent Configuration Parameters

Parameter	Description
enabled	Enables the Netflow exporter (Boolean).
ip	IP address of the Netflow collector.

Table 109. Netflow Agent Configuration Parameters (continued)

Parameter	Description
port	Port of the Netflow collector. The default is **2055**.
version	Netflow version (**1** | **5** | **9**). The default is **9**.
interval	Interval for which Netflow exports statistics (in seconds). The default is **10** seconds.
v9template	Number of Netflow packets sent before a version 9 template is sent. The default is **10** packets sent before a template is sent.

Netflow Filter Command

To configure the Netflow filters, enter the following command:

```
> config netflow filter
```

Table 110 describes the parameters for **config netflow filter**.

Table 110. Netflow Filter Configuration Parameters

Parameter	Description
sourceport	Source port to monitor.
destport	Destination port to monitor.
srcip	Source IP address to monitor.
dstip	Destination IP address to monitor.
tos	ToS tag value to monitor.
ipproto	IP protocol to monitor (**any**|**udp**|**tcp**|**icmp**). The default is **any**.
ethproto	Ethernet protocol to monitor (**ip**|**arp**|**rarp**).
srcmac	Source MAC address to monitor.
dstmac	Destination MAC address to monitor.
interface	Interface to monitor.

Netflow Configuration Example

This example configures Netflow as follows:

Netflow Collector location: 192.168.134.167, port 3000
Netflow version: 9
Traffic to be monitored: Traffic from IP address 10.0.1.100 and tagged with IP ToS value 248

```
> config netflow agent enabled yes ip 192.168.134.167 port
3000 version 9
*> config netflow filter srcip 10.0.1.100 tos 248
```

```
*> save
```

Show Netflow Status

To show the configuration and status of the Netflow agent, enter the following command:

```
> show netflow agent

Status:

   Enabled               yes
   Collector IP          192.168.134.167
   Collector Port        3000
   Version               9
   Export Interval       10
   V9 Template Interval  10
```

Show Netflow Filters

To show the Netflow filters, enter the following command:

```
> show netflow filter

Netflow Filter:

   Source Port     any
   Dest Port       any
   Source IP       10.0.1.100
   Dest IP         any
   ToS             248
   IP Proto        ANY
   Eth Proto       ANY
   Source MAC      ANY
   Dest MAC        ANY
   Interface       ANY
```

Show Netflow Statistics

To see statistics for Netflow exporter activity, enter the following command:

```
> stats netflow agent

Netflow Stats:

  Total sent flows                    0
  Total sent packets                  0
  Number of Active netflow flows      2
```

Clear Netflow Statistics

To clear the statistic counters kept for the Netflow exporter, enter the following command:

```
> clear netflow agent
```

SNMP Agent

The BSGX4e device implements an SNMP agent. Its Management Information Bases (MIB) are described in Internet Engineering Task Force (IETF) Request for Comments (RFC) 1213; SNMP traps are supported.

The SNMP agent replies only to SNMP version 2c requests. Apart from the system group, all MIBs are in read-only mode in this version; you cannot configure the BSGX4e through SNMP.

The SNMP agent sends the following traps:

- **ColdStart**: indicates the BSGX4e has restarted.
- **WarmStart**: indicates the SNMP agent has restarted.
- **LinkUp**: indicates an interface has come up.
- **LinkDown**: indicates an interface has gone down.
- **AuthenticationFail**: indicates SNMP authentication has failed (such as when the wrong community name is used).

NOTE: SNMP traps are sent on port 162; this cannot be configured. The port used by the SNMP agent must be open, allowing SNMP clients to reach it.

To configure the SNMP agent:

1. Ensure that the agent is enabled and configured as desired. (The default configuration enables the agent.)
2. Configure a community (or reconfigure the default communities).

NOTE: Two SNMP communities are configured by the default configuration: a read-only community named PlsChgMe!RO and a read-write community named PlsChgMe!RW. The default configuration does not configure IP addresses for the communities.

SNMP Configuration Command

To enable and configure the SNMP agent, enter the following command:

```
> config snmp agent
```

Table 111 describes the parameters for **config snmp agent**.

Table 111. SNMP Agent Configuration Parameters

Parameter	Description
enabled	Enables the agent (Boolean). The agent is initially enabled.
port	Port on which the agent listens. The default is port **161**.

Table 111. SNMP Agent Configuration Parameters (continued)

Parameter	Description
sysdesc	SNMP system description (sysDescr MIB).
sysloc	SNMP system location (sysLocation MIB)—physical location of the hardware. Empty when the hardware is shipped from the factory, this field is usually configured when the hardware is first installed.
syscon	SNMP system contact (sysContact MIB)—contact person for this hardware. Empty when the hardware is shipped from the factory, this field is usually configured when the hardware is first installed.
sysname	SNMP system name (sysName MIB)—administrator assigned to this hardware. Empty when the hardware is shipped from the factory, this field is usually configured when the hardware is first installed.

SNMP Community Command

To configure an SNMP community, enter the following command:

```
> config snmp community
```

Table 112 describes the parameters for **config snmp community**.

Table 112. SNMP Community Configuration Parameters

Parameter	Description
[community]	Name for the community access string.
ip	IP address of the management station.
access	Access rights for this community string (**read** | **read-write**).

NOTE: Two SNMP communities are configured by the default configuration: a read-only community named PlsChgMe!RO and a read-write community named PlsChgMe!RW. The default configuration does not configure IP addresses for the communities.

SNMP Agent Configuration Example

The following example starts the SNMP agent on port 161. It then configures an SNMP community, as follows:

SNMP community: `public`
Access MIBs: `read-only mode`
SNMP client IP address: `192.168.134.160`

```
> config snmp agent enabled yes port 161
*> config snmp community public ip 192.168.134.160 access
read
*> save
```

Show SNMP Agent Configuration

To show the configuration of the SNMP agent, enter the following command:

```
> show snmp agent

SNMP Agent:

   Enabled     on
   Port        161
   SysDesc     Nortel BSGX4e; SW version BSG T2 2.02.0227
   SysLoc
   SysCon
   SysName
```

Table 113 shows the relationship of the CLI data fields and SNMP group objects, and their access modes.

Table 113. SNMP Data Fields

CLI Data Field	SNMP Group Object	Access Mode
SysDesc	sysDescr	read-only
SysLoc	sysLocation	read-write
SysCon	sysContact	read-write
SysName	sysName	read-write

Show SNMP Community Configuration

To show the configuration of SNMP communities, enter the following command:

```
> show snmp community

SNMP Communities:

Community IP               Access
-----------------------------------------------------------
public    192.168.134.160  read
```

Show SNMP Agent Statistics

To see the statistics kept for the SNMP agent, enter the following command:

```
> stats snmp agent

Snmp Agent Stats

Out Pkts                405656          In Pkts                 402277
In BadCommunityNames         0             In BadVersions           0
In ASNParseErrs              0             In BadCommunityUses      0
In NoSuchNames               0             In TooBigs               0
In GenErrs                   0             In ReadOnlys             0
```

```
In TotalSetVars              0        In TotalReqVars         402277
In GetNexts             402277        In GetRequests          402277
In GetResponses              0            In SetRequests           0
Out TooBigs                  0            In Traps                 0
Out GenErrs                  0            Out NoSuchNames          0
Out GetNexts                 0            Out GetRequests          0
Out GetResponses             0            Out SetRequests          0
Enable AuthenTraps           1          Out Traps               3379
                                          Silent Drops             0
```

Table 114 describes the statistics of the SNMP agent.

Table 114. SNMP Agent Statistics

Statistic	Description
Out Pkts	Total number of Out SNMP messages.
In Pkts	Total number of In SNMP messages.
In BadCommunityNames	Total number of In messages with an unknown community name.
In BadVersions	Total number of In messages with an unsupported SNMP version.
In ASNParseErrs	Total number of In messages with ASN.1/BER errors.
In BadCommunityUses	Total number of In messages with a disallowed operation.
In NoSuchNames	Total number of In messages with *nosuchName* in error-status field.
In Toobigs	Total number of In messages with *tooBig* in error-status field.
In GenErrs	Total number of In messages with *genErr* in error-status field.
In ReadOnlys	Total number of In messages with *readOnly* in error-status field.
In TotalSetVars	Total number of Set-Request PDUs processed successfully.
In TotalReqVars	Total number of Get-Request and Get-Next PDUs.
In GetNexts	Total number of Get-Next PDUs.
In GetRequests	Total number of Get-Request PDUs.
In GetResponses	Total number of Get-Response PDUs.
In SetRequests	Total number of Set-Request PDUs.
Out TooBigs	Total number of Out Messages with *tooBig* in error-status field.
In Traps	Total number of SNMP Trap PDUs accepted and processed.
Out GenErrs	Total number of Out Messages with *genErr* in error-status field.

Table 114. SNMP Agent Statistics (continued)

Statistic	Description
`Out NoSuchNames`	Total number of Out Messages with *nosuchName* in error-status field.
`Out GetNexts`	Total SNMP Get-Next PDUs generated.
`Out GetRequests`	Total SNMP Get-Request PDUs generated.
`Out GetResponses`	Total SNMP Get-Response PDUs generated.
`Out SetRequests`	Total SNMP Set-Request PDUs generated.
`Enable AuthenTraps`	Permission to generate authentication-failure traps, enabled (1), disabled (2).
`Out Traps`	Total SNMP Traps generated.
`Silent Drops`	Total number of In PDUs silently dropped.

Clear SNMP Statistics

To clear the counters kept for SNMP statistics, enter the following command:

```
> clear snmp agent
```

SNMP Traps

NOTE: You must start the SNMP agent.

SNMP Trap Configuration Command

To enable and configure SNMP traps, enter the following command:

```
> config snmp traps
```

Table 115 describes the parameters for **`config snmp traps`**.

Table 115. SNMP Traps Configuration Parameters

Parameter	Description
`enabled`	Enables SNMP traps (Boolean)
`comm`	Traps community.
`ip`	IP address of the management station to receive traps.

SNMP Trap Configuration Example

The following example enables and configures the SNMP traps to be sent to IP address 192.168.134.161 for the *public* community:

```
> config snmp traps enabled yes comm public ip
192.168.134.161
*> save
```

Show SNMP Trap Configuration

To show the configuration of the SNMP traps, enter the following command:

```
> show snmp traps

SNMP Traps:

   Enabled     yes
   Comm        public
   IP          192.168.134.161
```

Copying Trap MIB Data

Use the maintenance command **trapmib** to display or store the contents of the *trap mib* file.

To display the trap mib file, enter the following command:

```
> trapmib
```

To copy the trap mib file to a file in the memory of the BSGX4e device, enter the file name on the command:

```
> trapmib flash <filename>
```

SNMP Trap Statistics

For more information about the SNMP trap statistics, see "Show SNMP Agent Statistics" (page 349). To clear the SNMP trap statistics of the SNMP traps, see "Clear SNMP Statistics" (page 351).

TCPdump Command

The maintenance command *tcpdump* displays network traffic received and transmitted by the BSGX4e device. The traffic is captured and displayed on the current session (console, Telnet, or SSH). Only traffic designated for the BSGX4e is captured. (TCPdump cannot be used as a promiscuous packet sniffer.)

CAUTION: TCPdump is intended to be used for problem investigation only. Its use can cause poor system performance.

NOTE: TCPdump does not capture VoIP media packets to avoid harming voice call quality.

TCPdump captures packets on the specified interface. You can only specify one interface.

TCPDump Command Options

Table 116 describes the options for TCPdump. For more information about TCPdump, see "TCPdump Expressions" (page 407).

Table 116. TCPDump Options

Option	Description
-c	Number of packets to display. Specify a count to limit the capture. Otherwise, enter **^C** to stop the capture.
-i	Interface for which traffic is displayed, such as eth0, eth1, or vif*n*.
-s	Number of data bytes to snarf snaplen from each packet. The default value is **68**.
-T	Forces the packets selected by *expression* to be interpreted as the specified type. Currently known types are **cnfp**, **rpc**, **rtp**, **rtcp**, **snmp,** and tftp.
-y	Data link type to use while capturing packets.
expression	Selects the packets to be dumped (see "TCPdump Expressions" (page 407)). If no expression is given, all packets are dumped.
-ADeflLNqR StuvxX	Specify one or more of these options to determine how information is displayed. **A:** Prints each packet in ASCII format, link level header not included. **x:** Prints each packet in hexadecimal format, link level header not included. The smaller of the entire packet or *snaplen* bytes are printed. **X:** Prints in both hexadecimal and ASCII formats. **q:** Quick format. Less protocol information is displayed. **v:** Verbose output. Printing includes time to live, identification, total length, and IP packet options. Packet integrity checks are enabled. **N:** Does not print domain names of host names. For example, instead of printing `nic.ddn.mil`, `nic` is printed. **t:** Does not print the time-stamp on each line. **l:** Buffers `stdout` lines; recommended when viewing data while it is captured.

Table 116. TCPDump Options (continued)

Option	Description
	D: Prints the list of network interfaces available on the system and on which interfaces **tcpdump** can capture packets. The number and interface name are printed, possibly followed by a text description of the interface. The interface name or number can be supplied to the **-i** option, which specifies on which interface to capture packets. **e:** Prints the link-level header on each dump line. **f:** Prints foreign Internet addresses numerically, instead of symbolically **S:** Prints absolute TCP sequence numbers. **u:** Prints undecoded Network File System (NFS) handles. **L:** Lists the known data link types for the interface and the exit. **R:** Assumes ESP packets are based on old specifications. (RFC1825 to RFC1829)

Limited Capture Example

The following example limits the packet captures to 10 packets on the eth0 interface:

```
> tcpdump -c 10 -i eth0

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes
16:16:11.294000 IP 192.168.22.60.1583 > 192.168.134.155.Telnet: . ack
2203345 win 65269
16:16:11.295000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
1:148(147) ack 0 win 17520
16:16:11.295000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
1:148(147) ack 0 win 17520
16:16:11.495000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
148:425(277) ack 0 win 17520
16:16:11.495000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
148:425(277) ack 0 win 17520
16:16:11.695000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
425:617(192) ack 0 win 17520
16:16:11.696000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
425:617(192) ack 0 win 17520
16:16:11.897000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
617:809(192) ack 0 win 17520
16:16:11.898000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
617:809(192) ack 0 win 17520
16:16:12.097000 IP 192.168.134.155.Telnet > 192.168.22.60.1583: P
809:1001(192) ack 0 win 17520

10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Unlimited Capture Example

If the capture is not limited by a packet count specified on the **-c** option, and you want to stop the capture, enter **^C** as shown below:

```
> tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size
68 bytes
16:16:11.294000 IP 192.168.22.60.1583 >
192.168.134.155.Telnet: . ack 2203345 win 65269
16:16:11.295000 IP 192.168.134.155.Telnet >
192.168.22.60.1583: P 1:148(147) ack 0 win 17520
16:16:11.295000 IP 192.168.134.155.Telnet >
192.168.22.60.1583: P 1:148(147) ack 0 win 17520
16:16:11.495000 IP 192.168.134.155.Telnet >
192.168.22.60.1583: P 148:425(277) ack 0 win 17520
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

Ping Command

This section describes how to use the `ping` command. This command is used to determine whether a particular device, such as a router or computer, is currently reachable across a network.

Table 117 describes the options for `ping`.

Table 117. Ping Options

Options	Description
destination	IP address or FQDN of the destination to ping.
-c	Number of ping requests to send; specifying **-c** without a count asks for unlimited ping requests.
-t	Total time (in seconds) before ending ping requests; specifying **-t** without a value asks for unlimited ping requests.
-i	Time interval (in milliseconds) between ping requests.
-l	Initial number of ping requests to send.
-f	Flood ping.
-p	Pattern to use (for example, FFFF).
-s	Number of data bytes to send.
-q	Completely quiet during ping.

Ping Example

The following example launches a ping to determine if 192.168.134.1 can be reached:

```
> ping 102.168.134.1

Pinging 192.168.134.1 (192.168.134.1): 56 data bytes

Reply from 192.168.134.1: bytes=56 icmp_seq=0 time<1ms
Reply from 192.168.134.1: bytes=56 icmp_seq=1 time=5ms
Reply from 192.168.134.1: bytes=56 icmp_seq=2 time<1ms
Reply from 192.168.134.1: bytes=56 icmp_seq=3 time<1ms

----- 192.168.134.1 ping statistics -----
4 packets transmitted, 4 packets received, 0.0% packet loss
Round-trip times: min/avg/max=0/0/5ms
```

Traceroute Command

The `traceroute` command is used to determine the path, in terms of router hops, taken to reach a certain device across a network.

NOTE: You must configure the firewall security policy to allow ICMP packets from any address (see "Firewall Security Policies" (page 130)). For example:

```
> config security policy new from eth0 to self proto icmp
```

Table 118 describes the options for `traceroute`.

Table 118. Traceroute Options

Option	Description
destination	IP address or FQDN of the destination to traceroute.
-w	Wait time (in seconds) for responding packets.
-m	Maximum number of hops to end trace.
-c	Number of packets for each hop.
-p	Port number to use.
-t	ToS tag value to use.
-S	Add the specified source address to the packets.
-v	Verbose output.
-r	Do not route.
-d	Do not resolve addresses to host names.

Traceroute Example

The following example launches a traceroute to determine the path to www.yahoo.com:

```
> traceroute www.yahoo.com

traceroute to www.yahoo.com (66.94.230.49), 30 hops max, 40 byte packets
 1  192.168.134.1 (192.168.134.1) 2.0 ms 2.0 ms 2.0 ms
 2  192.168.6.254 (192.168.6.254) 2.0 ms 3.0 ms 2.0 ms
 3  81.255.3.174 (81.255.3.174) 5.0 ms 3.0 ms 4.0 ms
 4  81.54.113.133 (81.54.113.133) 5.0 ms 4.0 ms 5.0 ms
 5  POS-1-1.MARG1.Marseille.transitip.raei.francetelecom.net (81.52.11.70)
9.0 ms 31.0 ms 9.0 ms
 6  POS-7-0.NCMAR301.Marseille.raei.francetelecom.net (193.253.14.97) 9.0
ms 31.0 ms 9.0 ms
 7  pos3-1.nrlyo201.Lyon.francetelecom.net (193.252.101.74) 13.0 ms 30.0 ms
13.0 ms
 8  pos12-0.ntaub301.Aubervilliers.francetelecom.net (193.252.103.78) 19.0
ms 19.0 ms 19.0 ms
 9  pos9-0.ntaub201.Aubervilliers.francetelecom.net (193.252.161.53) 19.0
ms 20.0 ms 47.0 ms
10  193.251.126.54 (193.251.126.54) 21.0 ms 25.0 ms 20.0 ms
11  po14-0.pascr3.Paris.opentransit.net (193.251.243.186) 20.0 ms 20.0 ms
21.0 ms
12  po14-0.ashcr1.Ashburn.opentransit.net (193.251.242.98) 271.0 ms 169.0
ms 147.0 ms
13  yahoo.GW.opentransit.net (193.251.254.126) 99.0 ms 108.0 ms 99.0 ms
14  so-3-1-0.pat2.pao.yahoo.com (216.115.101.130) 173.0 ms 180.0 ms 175.0
ms
15  ge-3-0-0-p241.msr1.scd.yahoo.com (216.115.106.179) 172.0 ms
ge-3-0-0-p251.msr2.scd.yahoo.com (216.115.106.183) 171.0 ms
ge-4-0-0-p441.msr1.scd.yahoo.com (216.115.106.203) 186.0 ms
16  ten-1-3-bas2.scd.yahoo.com (66.218.82.219) 173.0 ms
ten-2-3-bas2.scd.yahoo.com (66.218.82.223) 172.0 ms
ten-2-3-bas1.scd.yahoo.com (66.218.82.221) 171.0 ms
17  p18.www.scd.yahoo.com (66.94.230.49) 171.0 ms 171.0 ms 171.0 ms
```

19
SOFTWARE UPGRADES

This chapter provides information for upgrading the BSGX4e software. It describes:

- the file system and its navigation commands.
- how to save and restore the device configuration.
- how to upgrade the device software (application and/or bootloader):
  - using the Web user interface.
  - using an SFTP session.
- how to list the current configuration.

File System

The BSGX4e device is equipped with a compact flash memory of at least 128 Mb. A file system is provided to manage the information stored in the flash memory.

NOTE: If, while restarting, the device detects that no file system exists on the compact flash, the device automatically creates it.

The file system defines two main partitions:

- `/cf0usr` for user data.
- `/cf0sys` for system data.

IMPORTANT: The content of the /cf0sys partition is critical for normal operation. It is recommended that NO changes be made to it, except for recommended boot/firmware upgrades, configuration settings, and SSH/SSL key importation.

The application software is stored in file *app.bin*, and the bootloader software is stored in file *boot.bin*.

File System Navigation

This section describes commands to navigate the file system.

To print the name of the working directory (the current directory), enter:

```
> pwd
```

Both absolute and relative paths are supported.

To change the current directory, specify the directory on the following command:

```
> cd
```

Both absolute and relative paths are supported.

To list the contents of a directory, enter:

```
> ls
```

Both absolute and relative paths are supported.

Table 119 describes the ls options.

Table 119. Ls Configuration Options

Option	Description
-l	Prints details.
[filename1]	File or directory to print.
[filename2]	Other file or directory to print.

File System Navigation Example

The following example shows the current directory, changes it, and then lists it:

```
> pwd
/cf0usr
> cd /cf0sys
> ls -l
  size          date       time       name
--------       ------     ------    --------
    1024    AUG-28-2006  17:25:10   ssl                <DIR>
    1024    AUG-21-2006  17:25:10   ssh                <DIR>
    1024    AUG-21-2006  10:55:00   flash              <DIR>
```

File System Management

This section describes commands to manage files and directories.

To display the contents of a file, specify the file on the following command:

```
> cat
```

To copy the contents of a file, enter the following command with the source file to be copied and the destination file to be copied to:

```
> cp <sourcefile> <destinationfile>
```

To remove a file or directory, enter the following command:

```
> rm
```

Table 120 describes the parameters for rm.

Table 120. rm Parameters

Parameter	Description
-d	Specify if the object to remove is a directory.
path1	Object (file or directory) to remove.
[path2]	Object (file or directory) to remove.

To make one or more directories, specify one or more names on the following command:

```
> mkdir
```

To show the formatting of the compact flash memory, specify a partition (**usr**, **sys**, or **all**) on the following command:

```
> dosfs show
```

To reformat the compact flash memory, enter the following command:

```
> dosfs format
```

NOTE: All information is erased. The initial file system is restored after the device is restarted.

File System Management Examples

Example 1

The following example displays the details of the partition `/cf0usr`:

```
> dosfs show usr

DOSFS VOLUME
------------
volume descriptor ptr (pVolDesc):       0x85b6e3f0
cache block I/O descriptor ptr (pCbio): 0x85b6e6dc
auto disk check on mount:              DOS_CHK_REPAIR | DOS_CHK_VERB_SILENT
max # of simultaneously open files:     12
file descriptors in use:                0
# of different files in use:            0
# of descriptors for deleted files:     0
# of obsolete descriptors:              0

current volume configuration:
 - volume label:        /cf0usr ; (in boot sector:    euphoriarocks

 - volume Id:           0xbeef
 - total number of sectors:     177,344
 - bytes per sector:            512
 - # of sectors per cluster:    4
 - # of reserved sectors:       1
 - FAT entry size:              FAT16
 - # of sectors per FAT copy:   174
 - # of FAT table copies:       2
```

```
 - # of hidden sectors:         0
  - first cluster is in sector # 381
  - directory structure:         VFAT
  - root dir start sector:               349
  - # of sectors per root:               32
  - max # of entries in root:            512

 FAT handler information:
 ------------------------
  - allocation group size:       5 clusters

- free space on volume:        90,273,792 bytes
```

Example 2

The following example creates a directory and makes it the current directory, and then copies a file into a new file in the new directory:

```
> mkdir test
> cd test
> cp /cf0usr/textfile textfile
> ls
textfile
```

Software Upgrade Procedures

You can perform software upgrades of the application (image) and the bootloader code using the Web user interface (Web UI) or an SFTP/SSH session.

For an introduction to the Web UI, see Web User Interface on page 337. For more information about the Web server, see “Web Server” (page 38). For more information about the SSH server, see “SSH Server” (page 36).

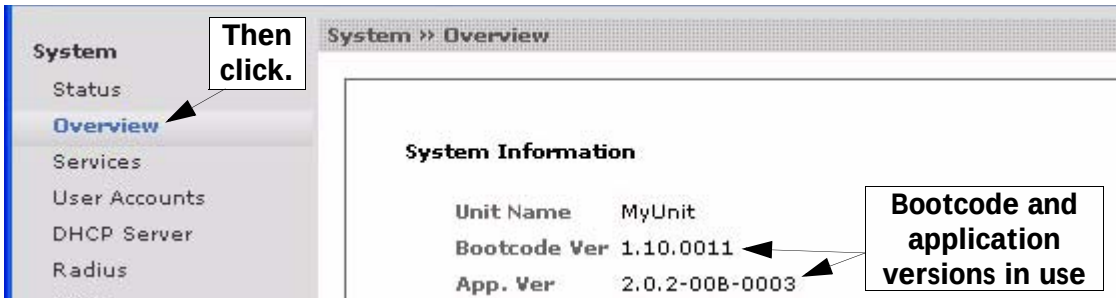
Device Software

The BSGX4e device stores two application software images, one in slot 1 and the other in slot 2 in its compact flash memory. This allows one image to be kept while the other image is being upgraded.

Each time the device is restarted, it reloads the *default* application image. When an application image is uploaded, it becomes the default image, unless you explicitly select the other image as the default. You can change the current default image at any time from the **Software Upgrade** screen (see “Change Default Application Image” (page 368)).

Check Current Software Versions

To see the software versions currently in use, select **System** on the top menu bar and then in the **System** menu in the left navigation pane, select **Overview**.



Web UI Upgrade Procedure

This section describes how to upgrade the application or bootloader software from a workstation on the Internet or on the LAN. It assumes that the BSGX4e is physically installed in the network and is operational.

Requirements

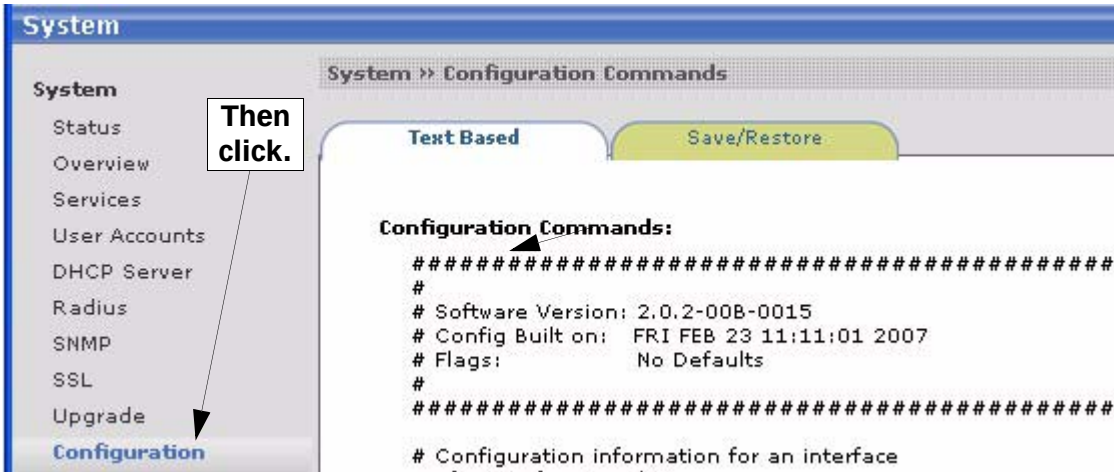
To upgrade the BSGX4e software using the Web UI, you must have the following:

- A workstation that can connect to the BSGX4e device using either one of the following Internet browsers: *Microsoft Internet Explorer* or *Mozilla FireFox*.
- The IP address of the BSGX4e device. If you connect from the WAN, use the eth0 address. If you connect from the LAN, use the eth1 address.
- The log on name and password for a user account that is configured on the device. The user account must have administrator capabilities, such as the default account **nnadmin**.
- The file containing the software upgrade must be on the workstation. The file location is entered during the upgrade procedure. You can select the file from the workstation directories by using the **Browse** button. To acquire the software file, contact your IT manager or "How to get help" (page 26).

Save the Current Configuration

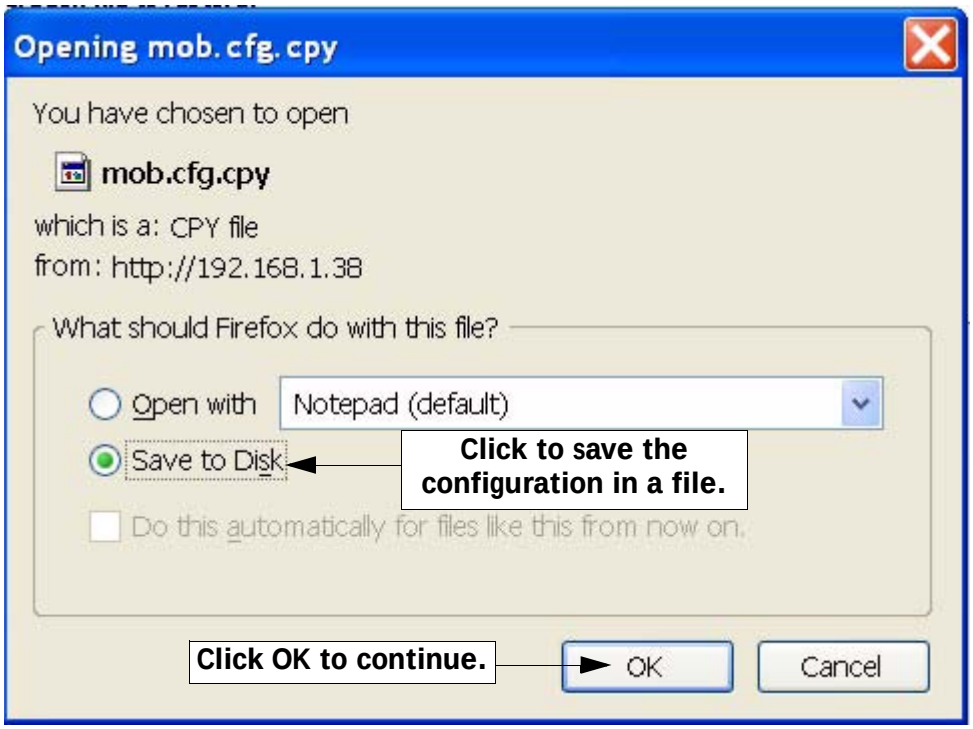
You can save the current device configuration and then restore it after a software upgrade.

1. **Log on to the Web user interface of the device. See "Logging on to the Web UI" (page 380).**
2. **Display the System Configuration screen by selecting System from the top menu bar and then from the System menu in the left navigation pane, select Configuration.**



3. **On the System Configuration screen, select the Save/Restore tab and then click Download.**

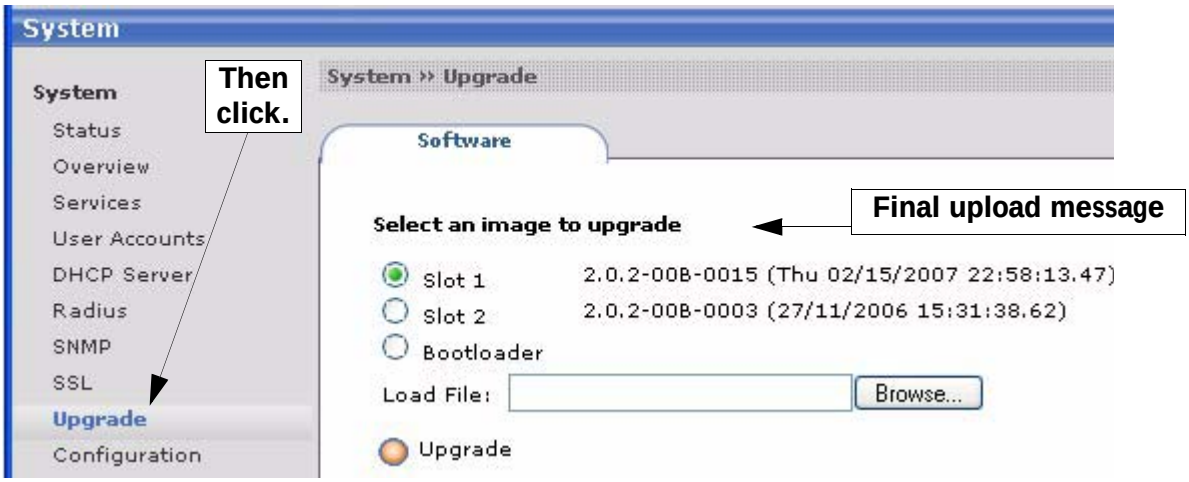
4. **The browser displays a window from which you can save the configuration file (*mob.ccfg.cpy*) to disk.**



5. **Click OK to save the file *mob.cfg.cpy* to disk. You can now perform a software upgrade (see "Upgrade Software through Web UI" (page 365)).**

Upgrade Software through Web UI

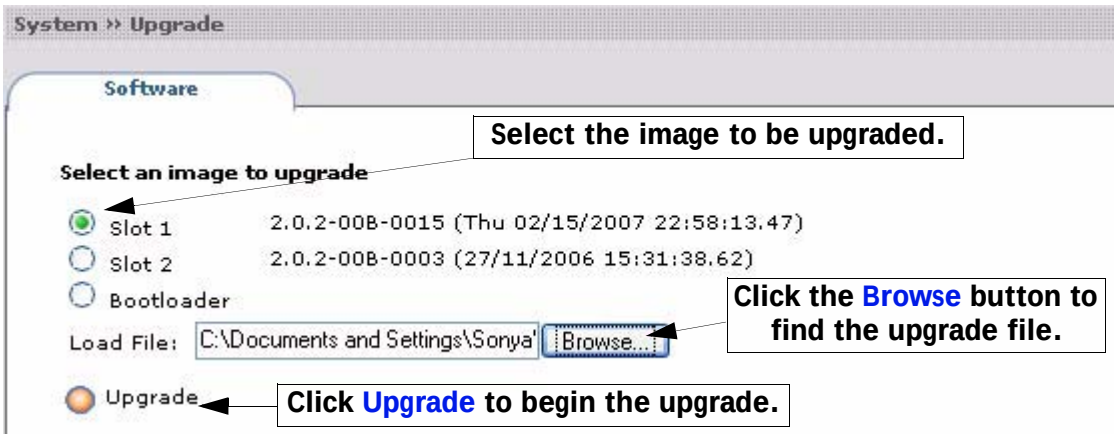
1. **Log on to the Web user interface of the device. See "Logging on to the Web UI" (page 380).**
2. **From the menu bar at the top of the screen, select System and then from the System menu in the left navigation pane select Upgrade.**



3. **In the upper half of the Software tab, select the software to be upgraded:**
   - **Slot 1** and **Slot 2** represent the application software images that are present in the BSGX4e unit.

     Note: The slot that is upgraded is automatically set as the default image that is run when the device restarts. You can change the default image after the upload. (see "Change Default Application Image" (page 368)).

   - **Bootloader** represents the application that loads in the new image.

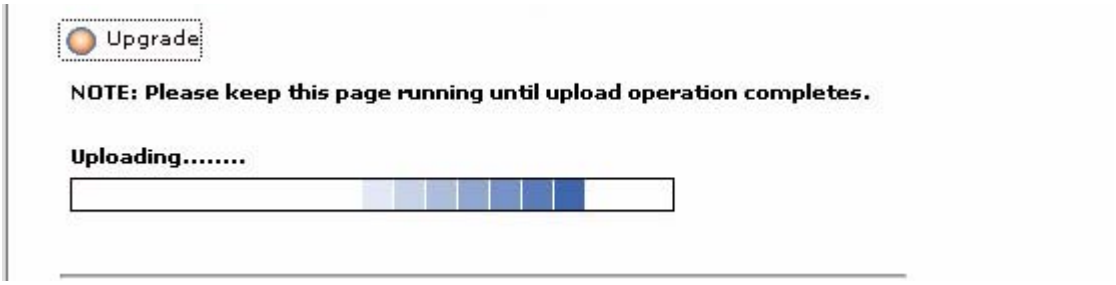


4. **In the Load File text box, enter the file to upload.**

   If necessary, use the *Browse* button to locate and select the file.

5. **Click Upgrade.**

   Messages are displayed as the upgrade steps complete.



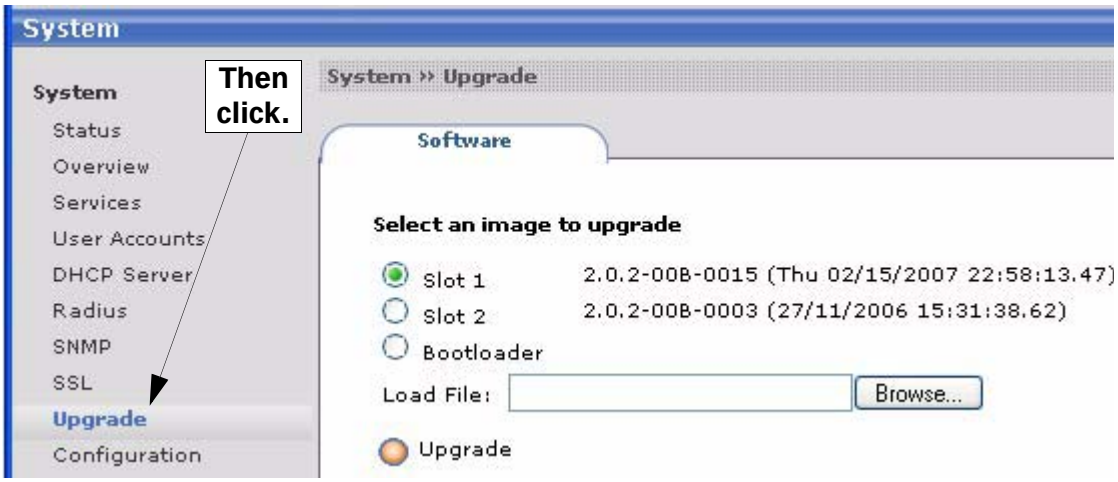
6. **When the upgrade is complete, a message directs you to reload the system.**

   IMPORTANT: Do not restart the device until after the message to reload the system appears.

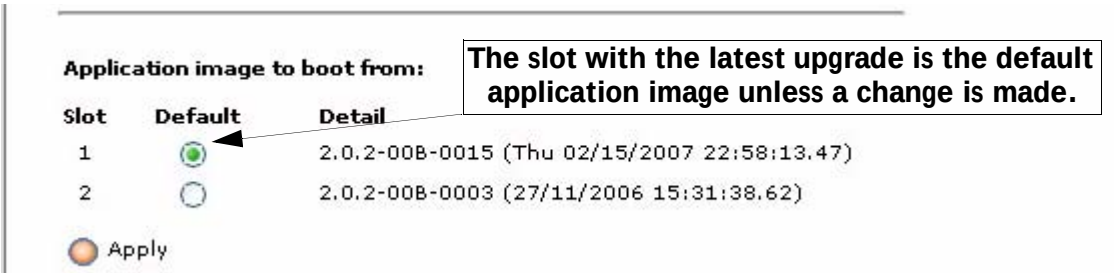
7. **To complete the upgrade, restart the device. To do so, under Operations in the lower left corner of the screen select Reload System.**

8. **When the unit restarts**, *the connection to the workstation is lost*. **Use your browser to reconnect to the unit and then log on again to verify the software upgrade.**

9. **On the menu bar at the top of the screen, in the left System menu select System and then click Upgrade.**

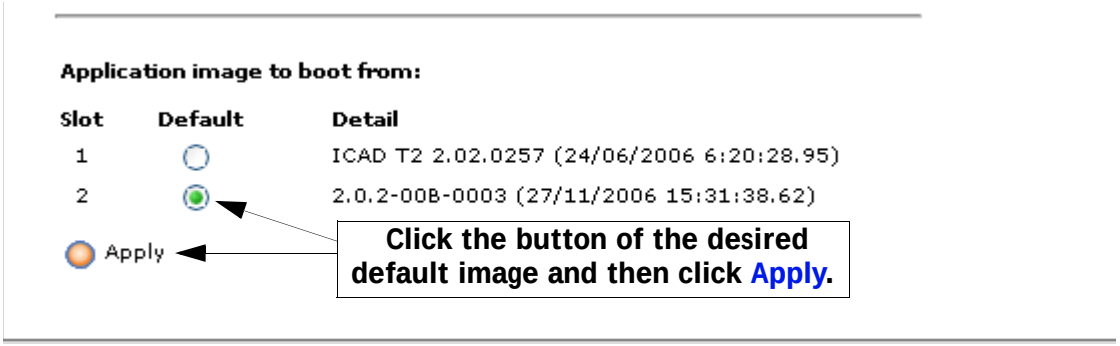


10. On the lower half of the Software Upgrade screen under **Application image to boot from**, the current image files are listed under **Detail**. The highlighted button under **Default** indicates which image is the current default.



Change Default Application Image

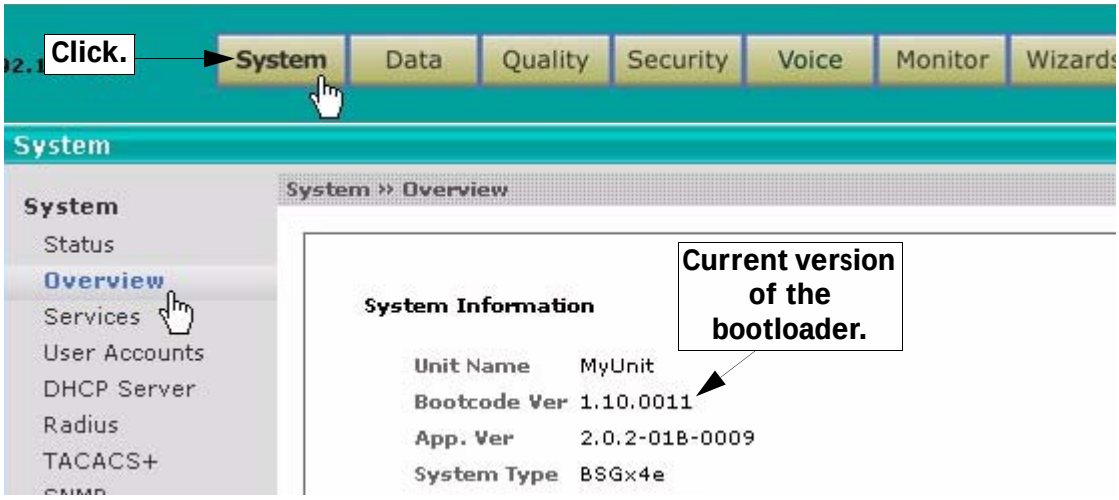
1. Display the Software Upgrade screen. (on the top menu bar, click **System** and in the left System menu click **Upgrade**)



2. **On the lower half of the screen under the heading Application image to boot from, click the button by the desired default image.**
3. **Click Apply.**

View Bootloader Version

1. **If you are already logged on, proceed to the next step. Otherwise, log on to the device through the Web UI. See "Logging on to the Web UI" (page 380).**
2. **On the menu bar at the top of the window, select System and then select Overview from the left menu.**

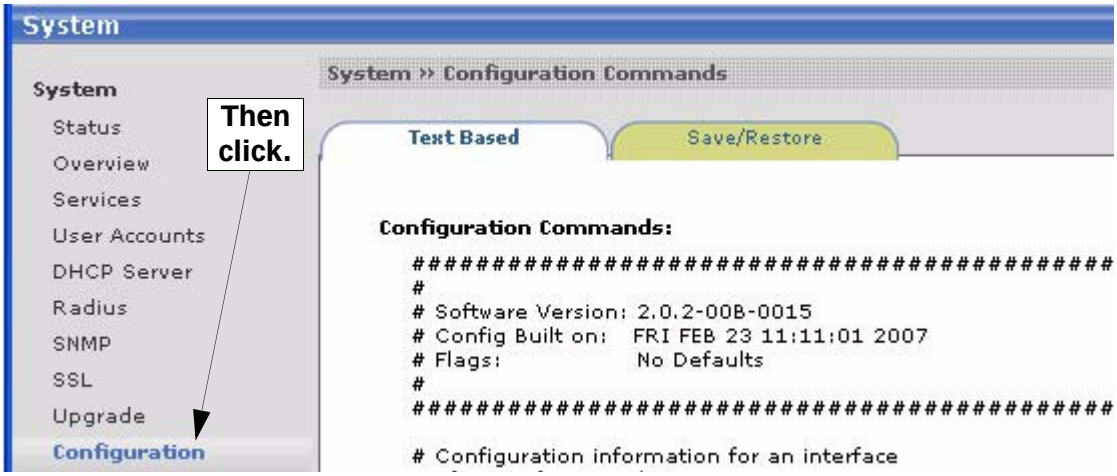


3. **The System Information section of the System Overview window shows the installed version of the bootloader software. The version of the default application is also shown.**

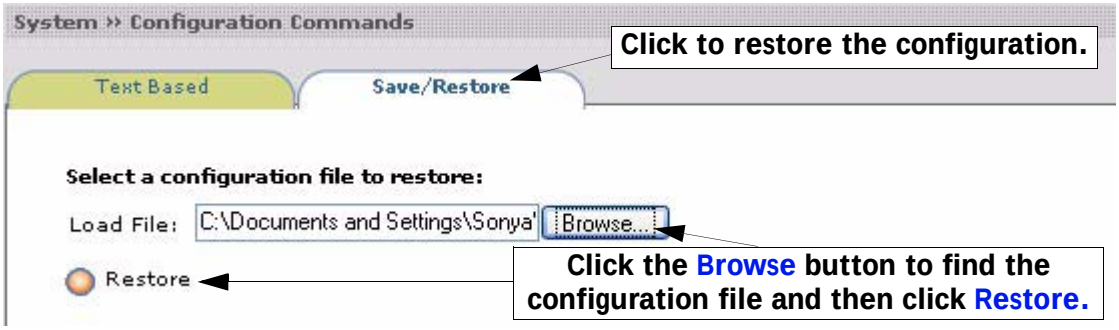
Restore the Configuration

After upgrading the device software, you can upload a device configuration file. You can use the configuration file saved before the software upgrade (**mob.cfg.cpy**) or another configuration file compatible with the current application software.

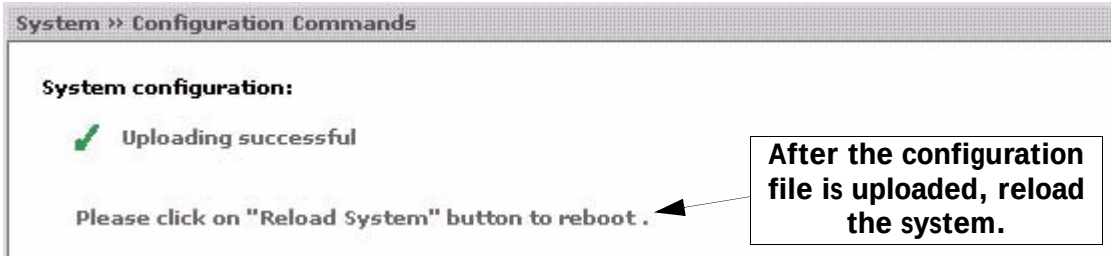
1. **Log on to the Web user interface of the device. See "Logging on to the Web UI" (page 380).**
2. **Display the System Configuration screen by selecting System from the top menu bar and then from the System menu in the left navigation pane, select Configuration.**



3. From the System Configuration screen, select the **Save/Restore** tab.
4. Click the **Browse** button and find the configuration file to be uploaded. To restore the configuration that was saved before the software upgrade, find the *mob.cfg.cpy* file .
5. Click the **Restore** button.



6. The configuration file is uploaded. When the upload is complete, you are directed to reload the system.


System » Configuration Commands
System configuration:
Uploading successful
Please click on "Reload System" button to reboot .
After the configuration file is uploaded, reload the system.

7. **To reload the system, in the Operations Menu in the lower left corner of the screen, click Reload System.**

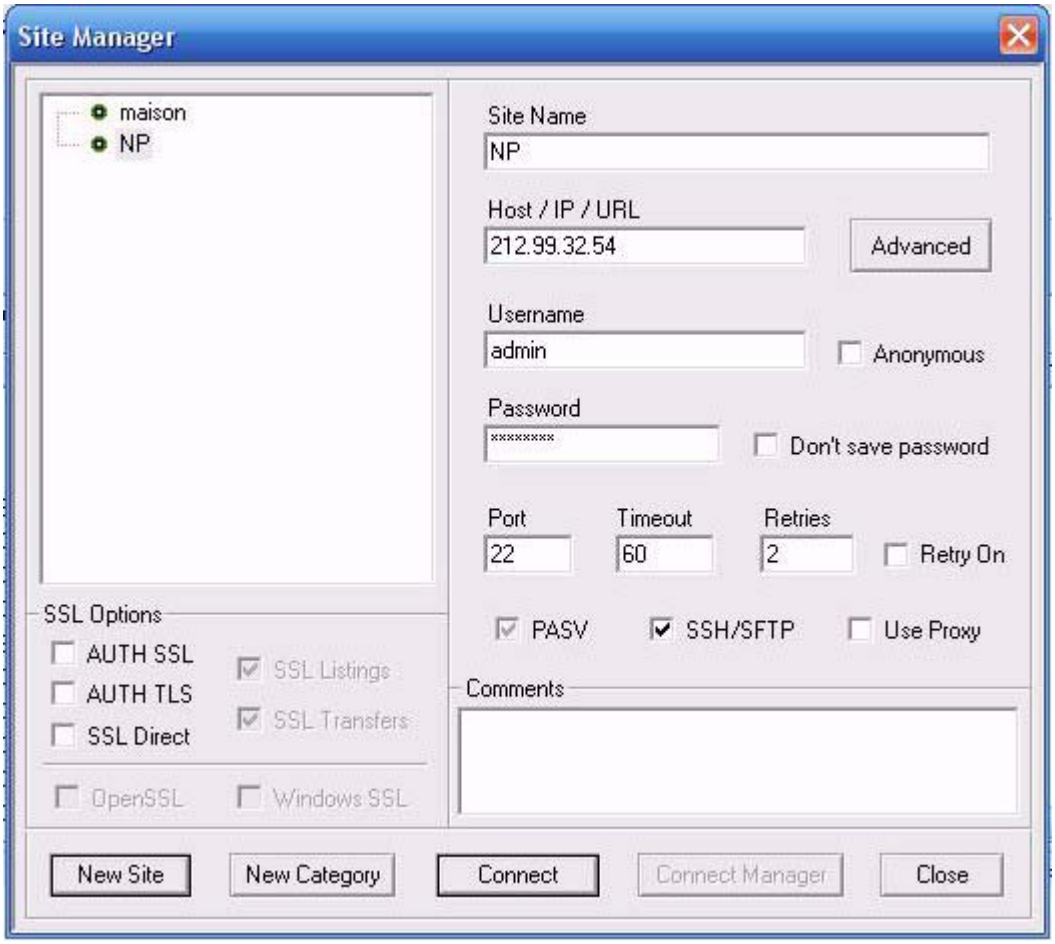
The reload sends the following message.

8. **The reload causes** *the connection to the workstation to be lost*. **If desired, use the browser to reconnect to the device.**

SFTP Upgrade Procedure

Upgrading software using an SFTP session:

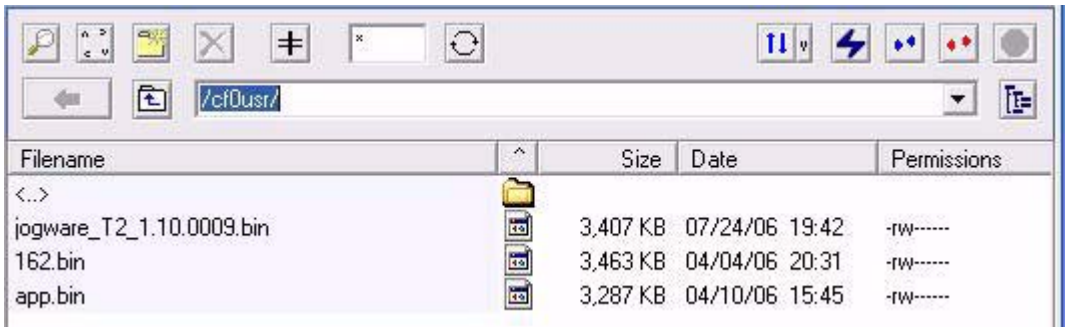
1. **Connect the SFTP server by using an SFTP client (such as CoreFTP).**



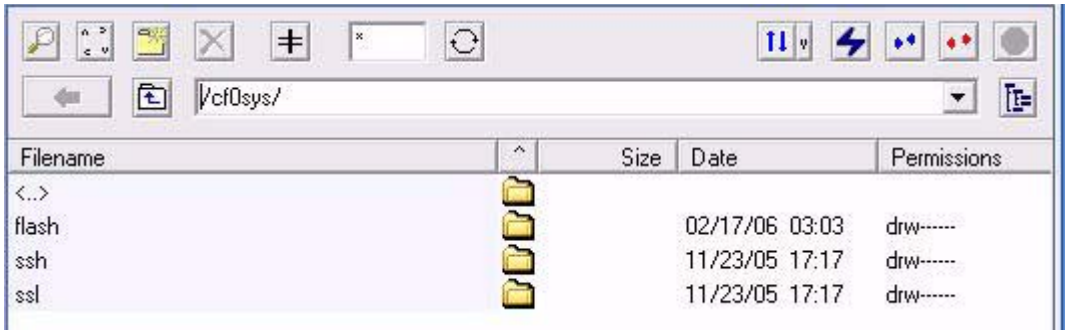
2. Click Yes to accept the SSH certificate.

The server's host key is not cached. There is no guarantee that the server is the computer you think it is.
The server's key fingerprint is:
ssh-dss 736 5a:73:15:64:61:f1:40:c9:bb:c9:d4:5b:8a:24:26:fa
If you trust this host, hit 'yes' to add the key to your SSH cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, enter 'no'.
If you do not trust this host, hit cancel to abandon the connection.
Store key in SSH cache?
Yes
No
Cancel

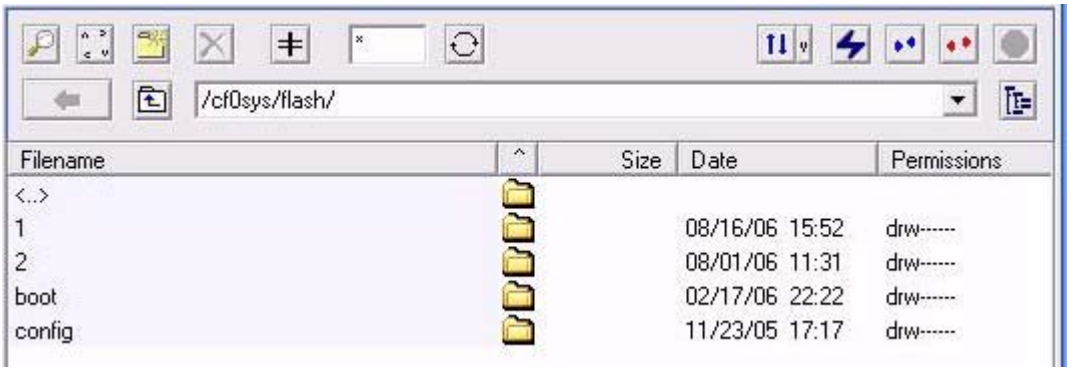
3. **The SFTP server is now connected.**



4. **Browse the server and go to /cf0sys.**



5. **Go in the directory flash.**

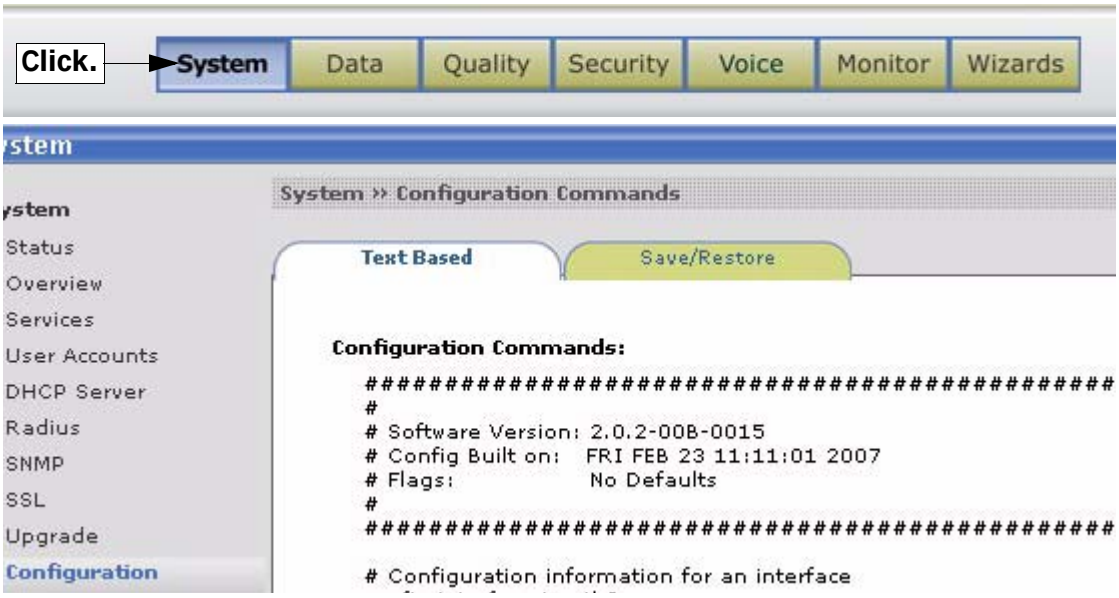


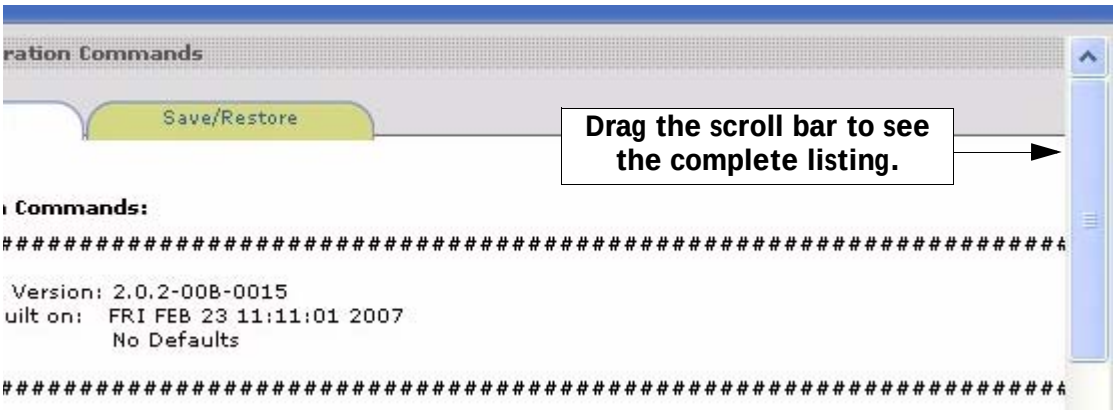
6. **Select the image to upgrade. To upgrade application image 1, go to directory 1. To upgrade application image 2, go to directory 2. To upgrade the bootloader, go to directory boot.**
7. **Rename the software upgrade file if needed. An application image must be file app.bin; a bootloader image must be file boot.bin.**
8. **Drag and drop the new application software.**
9. **Restart the unit.**

Listing the Configuration

To see the current configuration settings for a unit, do either of the following:

- Enter the **dump** command from a terminal session.
- Display the **System Configuration** screen from the Web UI in a browser session. To do this, select **System** from the top menu bar and then from the left menu select, **Configuration**.





The following is an example of a configuration listing:

```
Configuration Commands:
   ##########################################################################
   #
   # Software Version: 2.0.2-00B-0015
   # Config Built on:   FRI FEB 23 11:11:01 2007
   # Flags:             No Defaults
   #
   ##########################################################################

   # Configuration information for an interface
   config interface ip eth0
      ip 0.0.0.0
      dhcp on
   exit

   config interface ip eth1
      ip 192.168.1.38/255.255.255.0
      dhcp off
   exit

   # Configure the special system info attributes
   config system info
      unit MNUnit
   exit

   # Users groups management and configuration
   config user groups admins
      access ssh + web + cli + telnet + ftp
      all yes
   exit

   config user groups users
      access web + cli
   exit

   # User accounts for system access
   config user accounts admin
      access ssh + web + cli + telnet + ftp
      group1 admins
      group2 users
      group3 admins
      group4 admins
      group5 admins
      password ******
   exit

   config user accounts user
      access web + cli
      group2 users
      group3 users
      group4 users
      group5 users
      password ******
   exit

   # Rights for R/W access to elements
   config user rights admin
      access read + write
      gname admins
      object Admins
   exit

   config user rights useradv
      gname users
      object Admins
   exit
```

```
config user rights userbasic
   access read + write
   gname users
   object Users
exit

# Global setting of gain on all FXS circuits
config voice fxs gain Tx -6 Rx -6

# SIP Call Server configuration
config sip server settings Automatic
   Domain 10.10.10.14
exit

# Configure IKE parameters
config ike parameters LifeTime 86400 MaxLifeTime 259200

# Configure IPSEC parameters for IKE
config ipsec parameters LifeTime 28800 MaxLifeTime 86400 Group auto

# Configure where the system logger sends things to
config logging dest
   udpport
exit

# Quality of Service link settings
config qos link eth0 Max 100000000

# Setup the GoS 2.0 quality groups
config qos group Phone
   Committed 90000000
exit

# Display security policies for the system
config security policy new
   From eth0
   To self
   DPort 22
   Proto tcp
exit

config security policy new
   From eth0
   To self
   DPort 443
   Proto tcp
exit

config security policy new
   From eth0
   To self
   DPort 80
   Proto tcp
exit

config security policy new
   From eth0
   To self
   DPort 23
   Proto tcp
exit

config security policy new
   From eth1
   To eth0
exit

config security policy new
   From eth1
```

```
    To self
exit

# IDS Flood protection
config ids flood settings ah Threshold 100
config ids flood settings dhcp Threshold 10
config ids flood settings dns Threshold 20
config ids flood settings esp Threshold 100
config ids flood settings ike Threshold 100
config ids flood settings mgcp Threshold 255
config ids flood settings radius_1 Threshold 100
config ids flood settings radius_2 Threshold 100
config ids flood settings rip Threshold 20
config ids flood settings sip Threshold 255
config ids flood settings snmp Threshold 150
config ids flood settings sntp Threshold 10
config ids flood settings tftp Threshold 100
config ids flood settings unknown_IP_proto Threshold 500
config ids flood settings unknown_port Threshold 1000

# Voice media config for RTP port range and direct media usage
config media settings
    RTP 13000 - 14999
exit

# Numbering plan for voice application
config voice np *78
    Type Service
    Feature SDND
exit

config voice np *79
    Type Service
    Feature CDND
exit

config voice np *80
    Type Service
    Feature BXFER
exit

config voice np *90
    Type Service
    Feature SFWA
exit

config voice np *91
    Type Service
    Feature CFWA
exit

config voice np *93
    Type Service
    Feature SFWNA
exit

config voice np *94
    Type Service
    Feature CFWNA
exit

config voice np 1
    Length 9
    Prepend 0
exit

# SIP Session Controller Settings
config sip sc settings
    Server Automatic
    SigQoS Phone
```

```
exit

# Display Voice ACL policies
config voice acl new
   DeviceId SIP000F8F073088
   IP 10.0.1.100
   Type sip
   Action deny
exit

# Switch Port Based Priority Settings
config switch qos port 0-1 Priority LOWESTQ
config switch qos port 0-2 Priority LOWESTQ
config switch qos port 0-3 Priority LOWESTQ
config switch qos port 0-4 Priority LOWESTQ

# Switch QOS Type Setting
config switch qos setting Type Port

# IEEE 802.1p Priority Settings
config switch qos ieee 0 Priority LOWQ
config switch qos ieee 1 Priority LOWESTQ
config switch qos ieee 2 Priority LOWESTQ
config switch qos ieee 3 Priority LOWQ
config switch qos ieee 4 Priority HIGHQ
config switch qos ieee 5 Priority HIGHQ
config switch qos ieee 6 Priority HIGHESTQ
config switch qos ieee 7 Priority HIGHESTQ

# Whether to run Web server management interface
config service web Enabled yes

# Configure telnet access
config service telnet Enabled yes

# Configure ssh access
config service ssh AuthMethods "keyboard + password + publickey" Services "ssh + sftp"

# The Command Line Interpreter that interacts with the system
config shell terminal
   prompt ICAD
exit
```

A

WEB USER INTERFACE

This appendix introduces the Web User Interface (Web UI) for the BSGX4e device.

The Web UI is a graphic, full-screen interactive interface accessible through a Web browser. This allows for interactive administration and monitoring of device functions and it is accessed through either HTTP or HTTPS protocols. For more information about Web access, see "Web Server" (page 38).

NOTE: The Web UI supports most, but not all BSGX4e features. You must use CLI commands for some options.

Figure 18. Main Page

Web UI Features

This section summarizes the features of the Web UI.

- **Browser Support**

  The Web UI can be used through the following Web browsers:
  - Microsoft Internet Explorer (IE)
  - Mozilla FireFox

- **User Interface**

  The Web UI provides a visual and intuitive user interface. Options and information for each system area are shown as a separate screen. Functions are available by selecting (*clicking*) the desired feature.

- **Configuration**

  The Web UI supports the configuration of the following modules:
  - System
  - Data Interface
  - QoS
  - Security
  - VoIP

  For a configuration example, see "Configuration Example" (page 388).

- **Monitoring and Tracking**

  The Web UI can be used to monitor system operations and view statistical information.
  For a monitoring example, see "Monitoring Example" (page 390).

- **Wizards**

  The Web Wizards provide step-by-step guidelines for the following configurations:
  - WAN and LAN interfaces
  - VoIP session controller (either SIP or MGCP)
  - QoS policies for eth0 (WAN)
  - Firewall security policies
  - VoIP telephone interface for either SIP or MGCP
  - VPN tunnels

  For an example of using Wizards for configuration, see "Wizards Example" (page 391).

- **Software Upgrades**

  The Web UI makes it possible to upgrade the application and bootloader software in the unit. See "Web UI Upgrade Procedure" (page 363).

Logging on to the Web UI

This section describes how to access Web UI through the Internet. It assumes that the BSGX4e unit is installed in an IP network and is operational, that its WAN interface has an IP address, and that Web access has not been disabled.

Access Requirements

A Web UI log on has these requirements:

- A workstation set up to access the Internet. Its Web browser must be either Microsoft Internet Explorer or Mozilla FireFox
- The IP address of the BSGX4e device. From the LAN, use the eth1 address (default, 192.168.1.1); from the WAN, use the eth0 address.
- The name and password of a user account configured in the BSGX4e unit. Two user accounts are predefined: **nnadmin** with default password *PlsChgMe!* and **user** with default password *netcat*. See "User Management" (page 57).

Log on Procedure

1. **Enter the IP address from the Web browser:**
   For example, assuming that the eth1 IP address has not be changed from its default, enter the following to log on from a workstation on the LAN:

- **through HTTP**
  http://192.168.1.1
- **through HTTPS**
  https://192.168.1.1

2. **The log on window appears, requesting a user name and password. See Figure 19.**

Figure 19. log on Window

3. **Enter a user name and password in the text boxes.**
   The initial password for the predefined user account **nnadmin** is *PlsChgMe!*.
   Note: Names and passwords are case-sensitive.

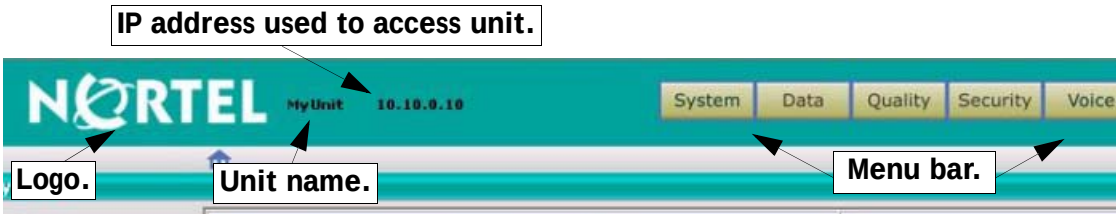
4. **Click Login.**
   The Web UI opens its System Screen, which shows current system statistics. See Figure 18.

Web UI Screen Structure

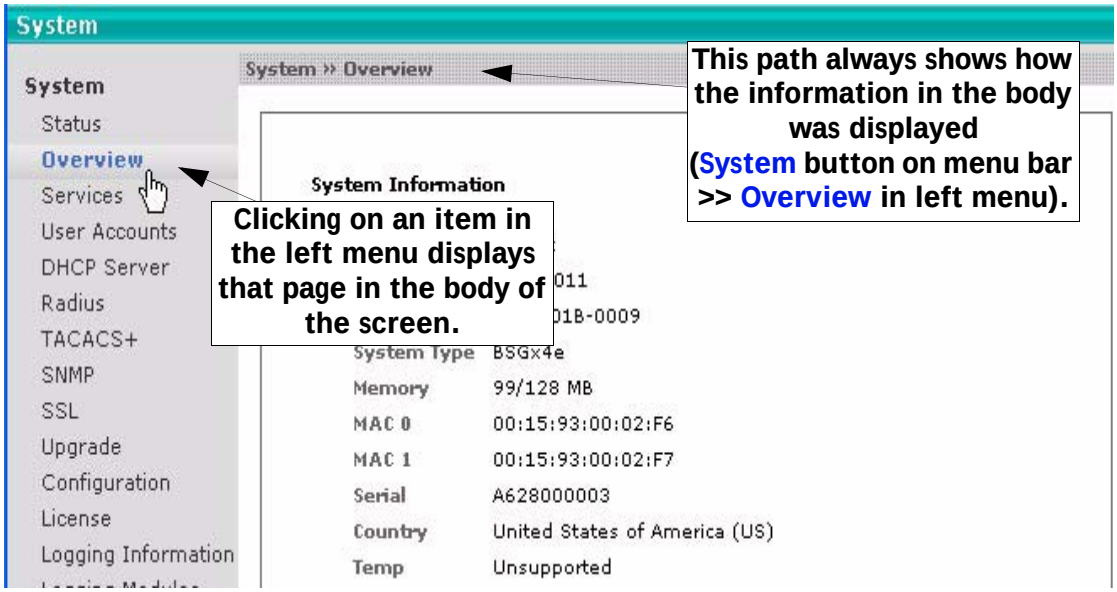
This section describes the structure of the Web UI screens, including the menu bar, help icons, and left side menu.

Menus

The strip at the top of every WebUI screen identifies the unit and displays a menu bar.



Each button on the menu bar displays a menu of links on the left side of the screen. The Web UI opens with the **System** menu displayed.



Help Icons

The narrow strip below the menu bar displays several icons:

- **Home**: Clicking on the house icon returns you to the home page (the **System Status** page).

- **Information**: Clicking on the **i** icon opens a second web page to an informational site.
- **Help**: Clicking on the **?** provides a summary of Web UI capabilities.
- **User Mode**: Clicking on **S/A** selects the desired user mode. Click on **S** for simple mode, in which field explanations are provided. Click on **A** for advanced mode; field explanations are not provided.

Operations Menu

The **Operations** menu is shown in the lower left corner of the screen. Its options determine the results of the Web UI session.

NOTE: Configuration changes take effect immediately. While using the Web UI, a change takes effect when you click the **Update** *or* **Apply** *button. However, the* **Update** *or* **Apply** *does not store the change in nonvolatile memory; unsaved changes are lost by a unit reload.*

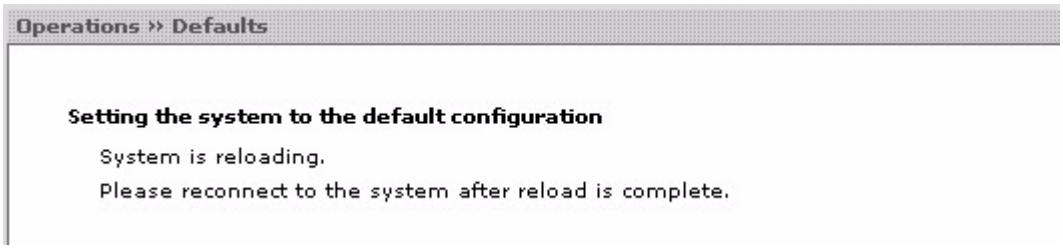
The **Operations** menu option you select determines if changes are kept and how the session ends.

- **Log Out**

  Logs out the user and returns to the login screen. Unsaved configuration changes are kept unless the unit restarts.
- **Save System**

  Saves configuration changes to nonvolatile memory. (When configuration changes are pending, the **Save System** button changes color.)
- **Defaults**

  Erases the current configuration and restores the original, default configuration of the unit. After confirmation, the following message appears and the unit disconnects from the browser.


Operations » Defaults
Setting the system to the default configuration
System is reloading.
Please reconnect to the system after reload is complete.

Note: After the default configuration is reloaded, all IP addresses are reset to their default values. For a browser to connect to the eth1 interface from the LAN, it must use the default IP address 192.168.1.1. If the browser cannot connect to the default IP address, then the IP address must be reset from the other interface or from a console session.

Note: After the default configuration is reloaded, the only valid user accounts are the two default accounts: **nnadmin** *with password* **PlsChgMe!** *and* **user** *with password* **netcat***.*

- **Reload System**

  Logs off the user and restarts the BSGX4e unit. Any unsaved configuration changes are discarded and the browser connection to the unit is lost. To begin a new Web UI session, enter the device IP address to reconnect the browser to the unit; the Web UI logon window then appears.

Web UI Menus

To display a Web UI page, you make two menu selections. First, you click a button on the top menu bar (see Figure 20) to display the corresponding menu on the left side of the screen. For example, if you click the **System** button, the **System** menu is displayed. Then you select a entry on the left menu to display a page of information.

Figure 20. Menu Bar

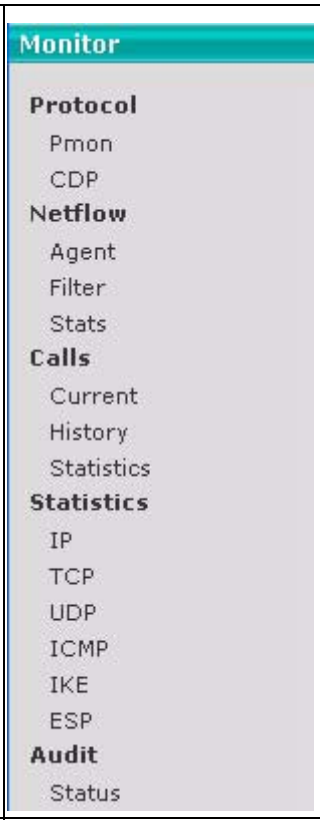
Table 121. Web UI Menus

▪ **System** System operations, including services, user accounts, DHCP, RADIUS, TACACS+, SNMP, SSL. From this menu, you can perform software upgrades and list the existing configuration. You can also change the messages logged and their destinations.	
▪ **Data** Data interfaces, relays, IP routing, and the LAN switch, including layer 2 QoS.	

Table 121. Web UI Menus

▪ **Quality** Features to ensure quality service, including Call Quality Monitoring, and configuration of Layer 3 GoS (Guarantee of Service).	
▪ **Security** Security services, including firewall policies, NAT, ALG, IDS (Intrusion Detection Service), and Voice ACL (Access Control List), and VPN configuration (IPSec and IKE).	
▪ **Voice** Voice services, including media settings, the session controller (SIP and MGCP), User Agent (also know as the Integrated Gateway) that provides VoIP access for analog devices, and Local Call Routing.	

Table 121. Web UI Menus

▪ **Monitor** Performance and activity information: the PMon (Protocol Monitoring) tool, CDP (Cisco Discovery Protocol), Netflow monitoring, call statistics, packet statistics for each protocol, and audit logging.	
▪ **Wizards** A wizard is a step-by-step configuration guide. Wizards are available to configure data interfaces, Quality of Service (GoS), the session controller (MGCP and SIP), firewall policies, VoIP phones. and VPNs.	

Configuration Example

The following section shows an example of configuration using the Web UI. The example configures a new user account. For more information about configuring User Accounts, see “User Accounts” (page 61).

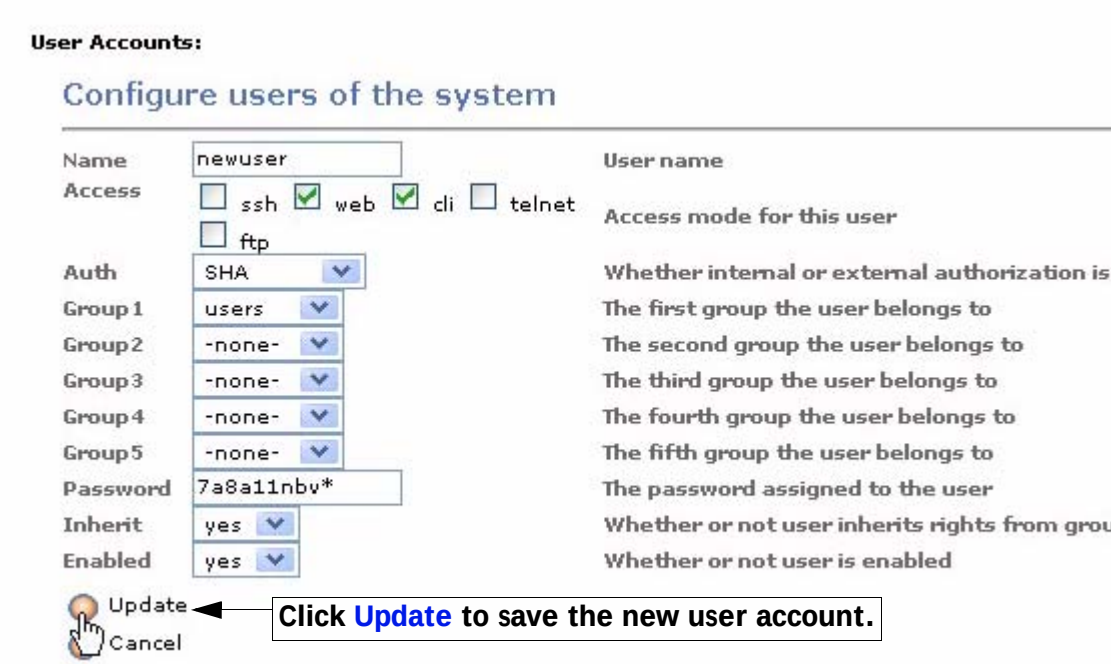
1. **From the menu bar at the top of the screen, select System.**

2. **From the System menu on the left of the screen, select User Accounts.**

3. **The User Accounts tabs are displayed in the body of the screen. The *Users* tab lists the existing user accounts.**

4. **To create a new user account, select the New button at the bottom of the tab.**

5. **Next, a form appears listing the options for the new user account. In the text box next to Name, enter the name of the new user account.**

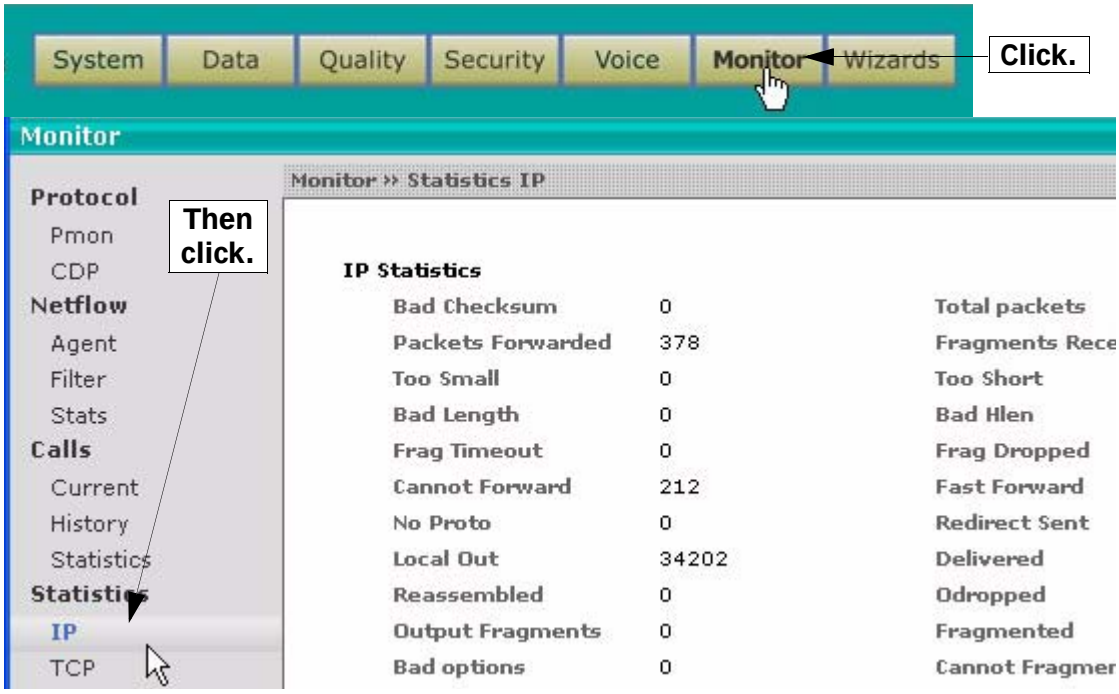


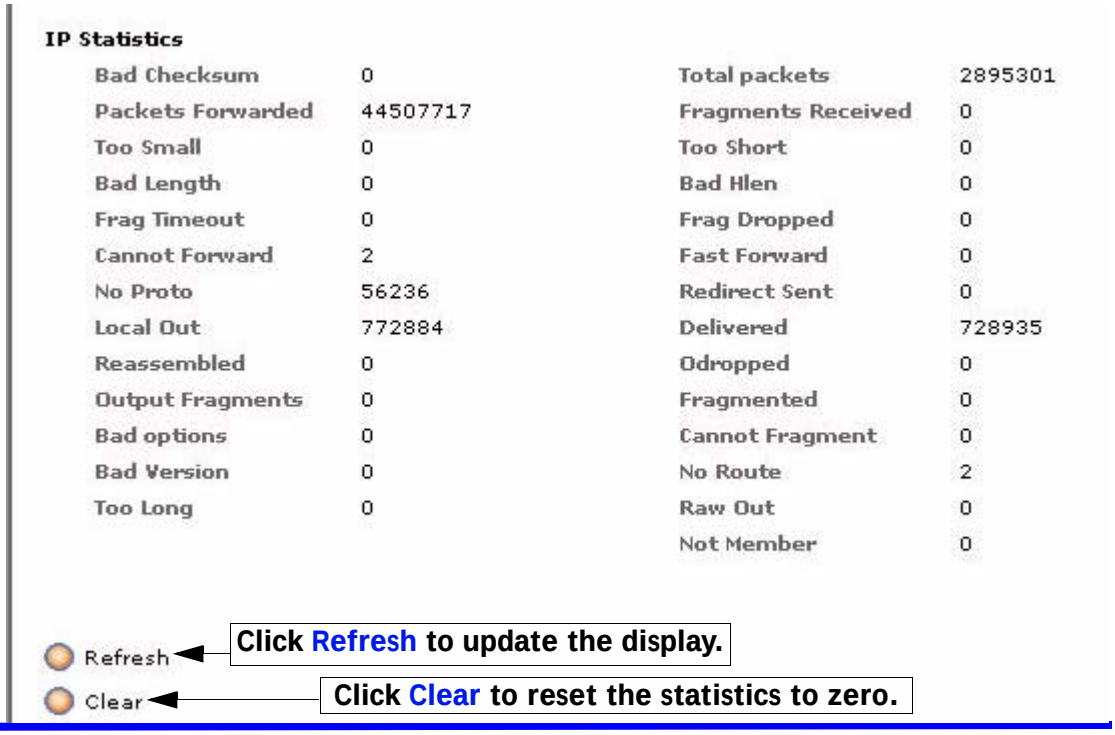
6. **Select the appropriate options for the new user. (Pull-down menus list the available options):**
   - **Access:** Check the access methods that the user account should be allowed.
   - **Auth:** Select the authentication method.
   - **Group1 – Group 5:** Select the user groups to which the account belongs.
   - **Password**: If the account uses internal authentication, enter its initial password.
   - **Inherit:** Select **yes** if the user inherits the permissions of the selected **Group**.
   - **Enabled:** Select **yes** or **no.** The user account cannot log in until it is enabled.
7. **Select Update.**
8. **To save the user account configuration, press the button Save Changes from the Operations menu in the lower left corner of the screen.**

Monitoring Example

The following example shows how to monitor IP statistics from the Web UI.

1. **On the menu bar at the top of the screen, select Monitor and then, from the Monitor menu on the left of the screen, under Statistics, select IP.**

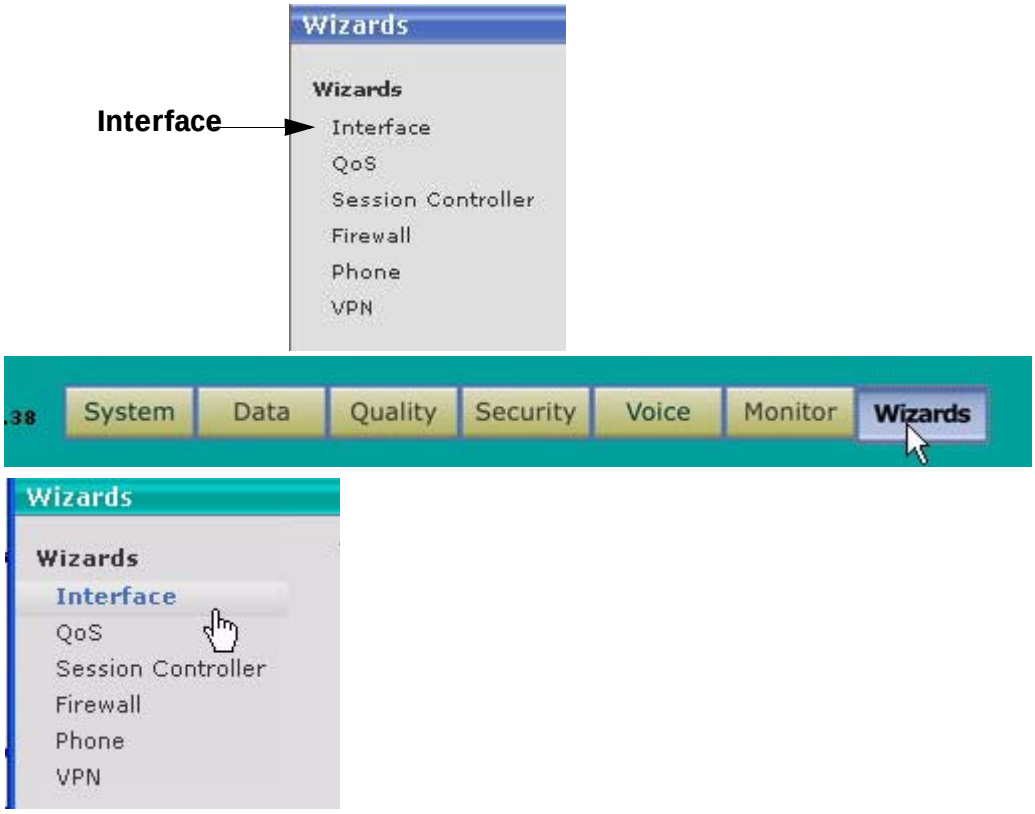



IP Statistics
Bad Checksum 0 Total packets 2895301
Packets Forwarded 44507717 Fragments Received 0
Too Small 0 Too Short 0
Bad Length 0 Bad Hlen 0
Frag Timeout 0 Frag Dropped 0
Cannot Forward 2 Fast Forward 0
No Proto 56236 Redirect Sent 0
Local Out 772884 Delivered 728935
Reassembled 0 Odropped 0
Output Fragments 0 Fragmented 0
Bad options 0 Cannot Fragment 0
Bad Version 0 No Route 2
Too Long 0 Raw Out 0
Not Member 0
Refresh
Click Refresh to update the display.
Clear
Click Clear to reset the statistics to zero.

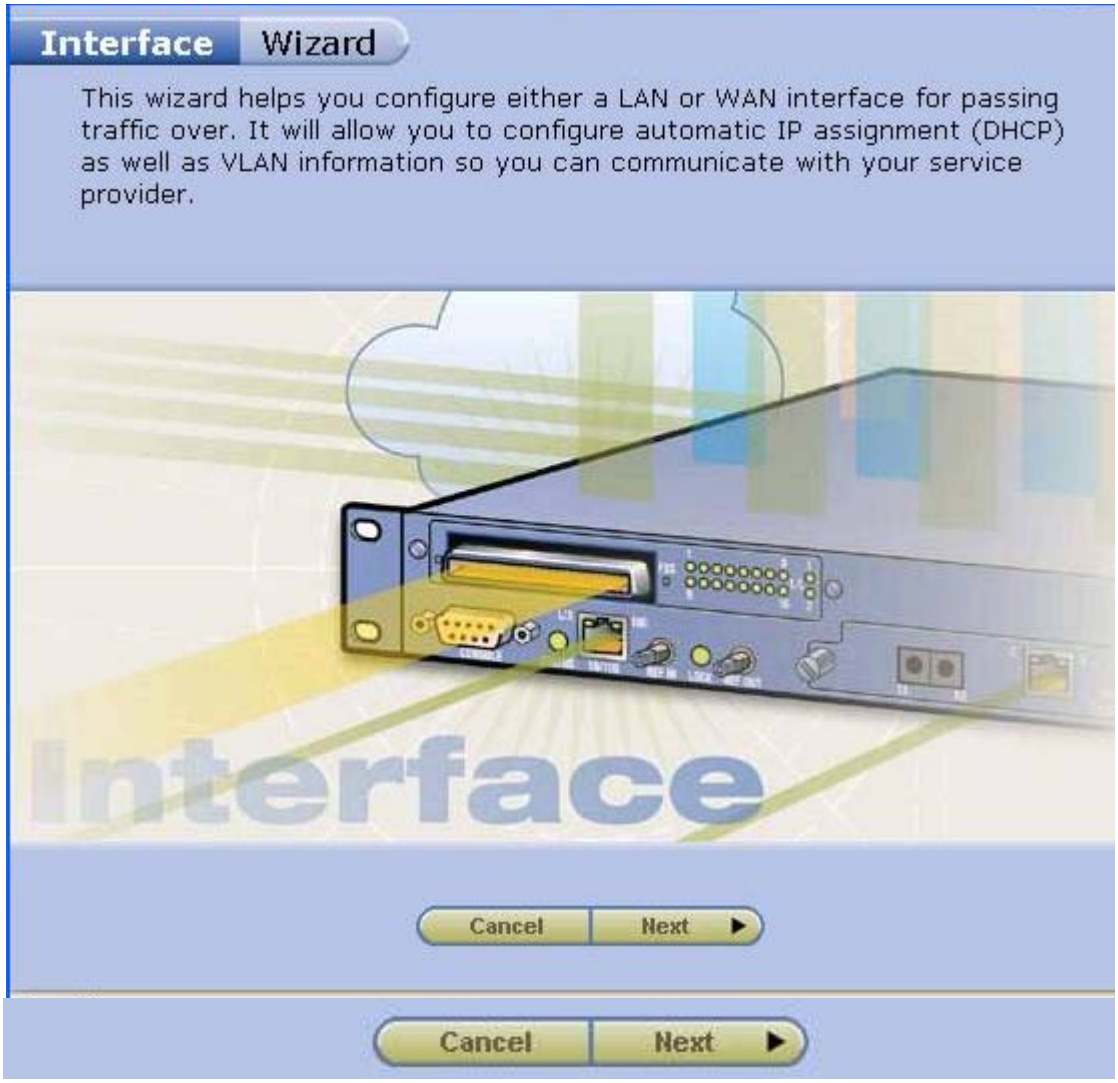
Wizards Example

This section shows an example of using a Wizard to configure a data interface.

1. **On the menu bar at the top of the screen, select the Wizards button and then select Interface in the left Wizards menu.**



2. **The first window summarizes interface configuration. To start the configuration, click Next.**

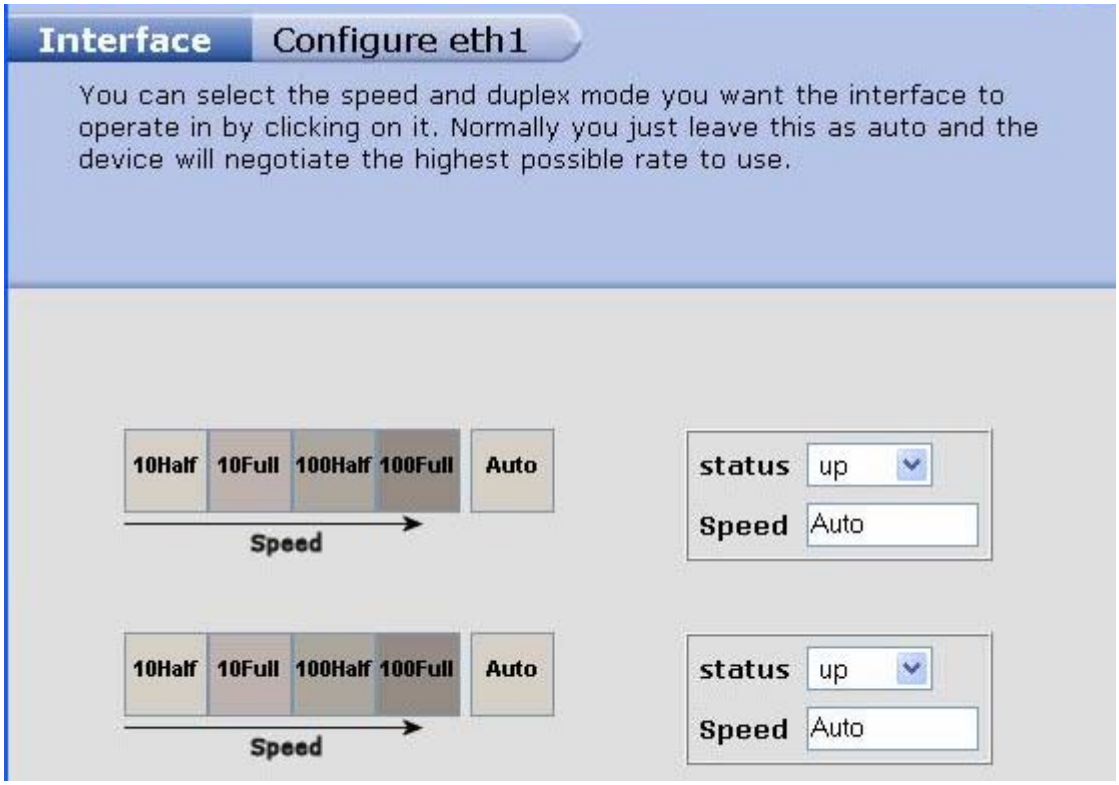

Interface Wizard
This wizard helps you configure either a LAN or WAN interface for passing traffic over. It will allow you to configure automatic IP assignment (DHCP) as well as VLAN information so you can communicate with your service provider.
Interface
Cancel
Next
Cancel
Next

3. **The next window offers a choice of interfaces. For this example, select the LAN button. Then press the Next button at the bottom of the window.**

4. **In the next window, select the LAN Ethernet interface eth1. Then press the Next button at the bottom of the window.**

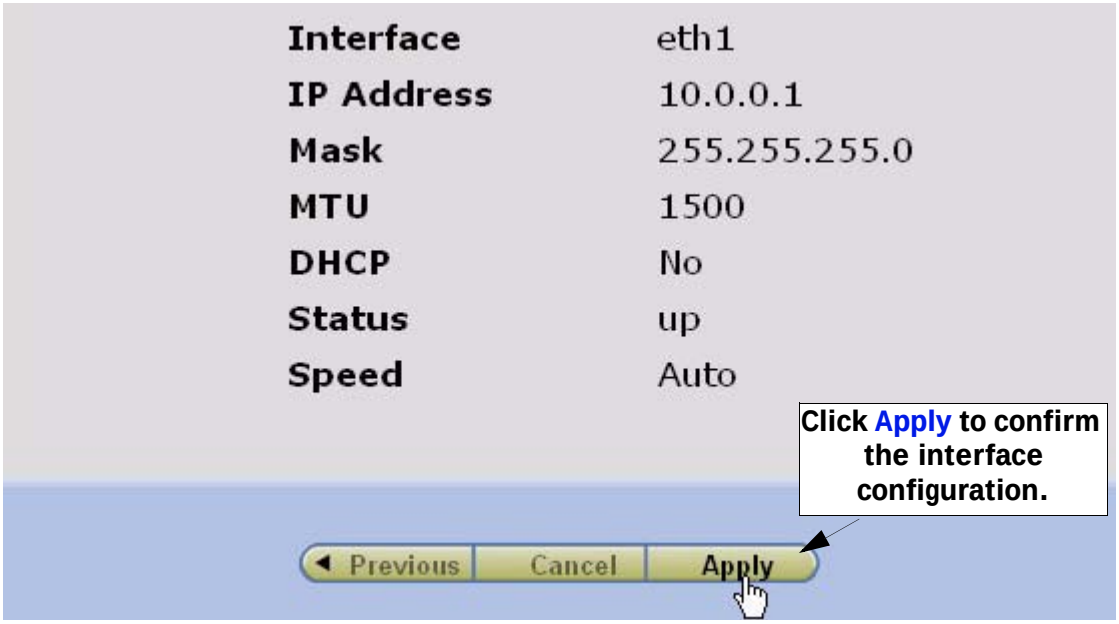
5. **Enter the IP address information and then press Next.**
   - **DHCP**: If a DHCP server can provide the IP address, select **yes.**
   - Otherwise, enter the **IP Address** and **IP Mask** values.

6. **On the next window, select the status (up or down) and the Speed option and then press Next.**



n

7. **To complete the configuration, verify the configuration options.**

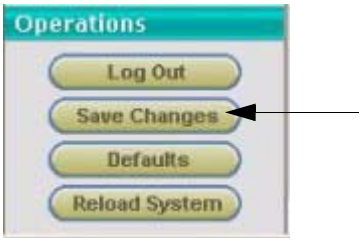


8. If the configuration is correct and should take place, select **Apply**. Otherwise:
   - Select **Previous** one or more times to display the previous windows and edit any settings.
   - Select **Cancel** to cancel the configuration change.
9. On the final window, click **Finish** to return to the Web UI screen.

Interface Wizard
Congratulations. You just completed the configuration of Interface eth1. Click the finish button to close the window.
Finish

10. The interface configuration takes effect as soon as the **Apply** button is clicked. However, at this point, the configuration changes have not been written to nonvolatile memory. If the unit restarts, the Wizard changes (and all other pending configuration changes) are lost.

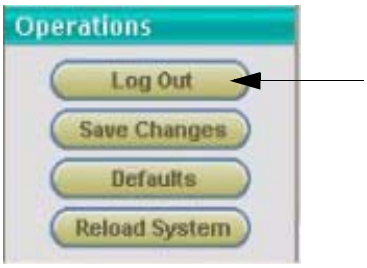
    To save the pending changes to nonvolatile memory, click **Save Changes** in the **Operations** menu in the lower left corner of the screen.


Operations
Log Out
Save Changes
Defaults
Reload System

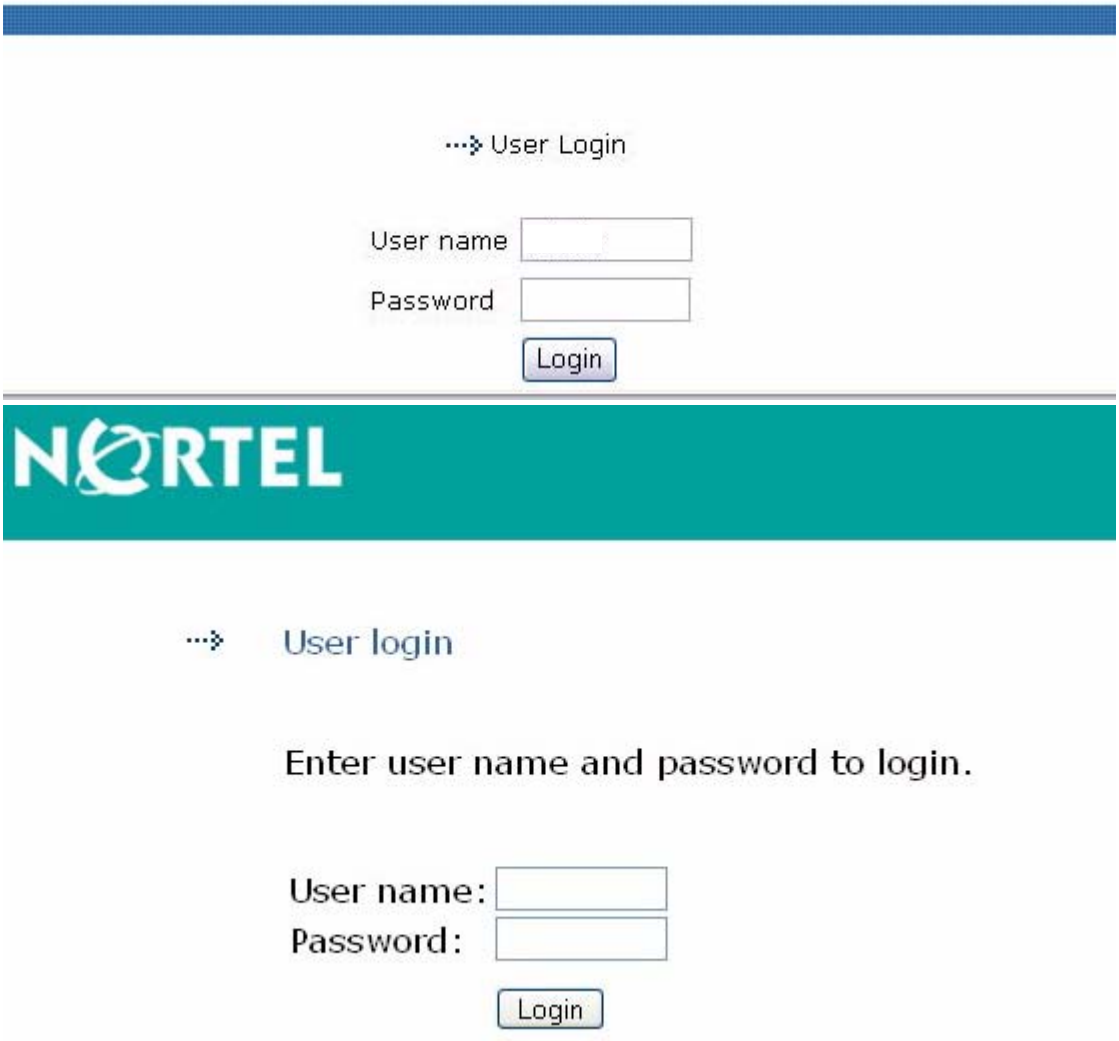
Exit Web UI

To ensure a secure system, log out of the Web UI when your work is complete.

1. **To exit the Web UI, select the Log Out button in the Operations menu in the lower left corner of the screen.**



2. **The login screen appears.**



3. **Close the Web browser and logout is complete.**

B
THIRD PARTY SOFTWARE

This appendix provides information about third-party software that you can use with the device. This software can be useful for installation, configuration, and the reading of files.

Software Applications

- **Acrobat Reader**
  www.acrobat.com
  Used for reading the PDF files provided on the CD that is shipped with the BSGX4e.

- **DHCP server**
  http://tftpd32.jounin.net/
  Used for software installation through network connection. This application also provides TFTP server functionality.

- **Telnet/SSH Client (PuTTY)**
  www.chiark.greenend.org.uk/~sgtatham/putty/
  Used for remote access to a computer through network connection.

- **PuTTY**
  www.chiark.greenend.org.uk/~sgtatham/putty/
  A telnet/SSH client.
  A tool for remote access to a BSGX4e.

- **Tera Term Pro**
  http://hp.vector.co.jp/authors/VA002416/teraterm.html
  Used for logging on to the BSGX4e.
  Used for software installation, configuration, monitoring, and viewing statistics.

- **TFTP server**
  http://tftpd32.jounin.net/
  Used for software installation through network connection. This application also provides DHCP server functionality.

- **WinSCP3**
  http://winscp.net/eng/index.php

Used for local software installation.
WinSCP is an open source SFTP client for Windows. Its main function is to secure file transfer between a local computer and a remote computer by using SSH.

C SSH FUNCTIONALITY

This chapter provides information about the SSH server, SFTP, and the subsystems SSH-TRANS, SSH-AUTH, and SSH-CONNECT.

Introduction

SSH provides secure Internet access to the BSGX4e CLI, which enables system administration to log on remotely, and securely configure and monitor the BSGX4e over an insecure network.

SSH consists of three components:

- The Transport Layer Protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity. As an option, compression can be provided. SSH-TRANS is usually run over a TCP/IP connection, but it can also run over any other reliable data stream.
- The User Authentication Protocol [SSH-AUTH] authenticates the client-side user to the server. SSH-AUTH runs over the transport layer protocol.
- The Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels. SSH-CONNECT runs over the user authentication protocol.

The SSH authentication process proceeds as follows:

- The client sends a service request a secure transport layer connection is established.
- A second service request is sent after user authentication is complete.
- New protocols are defined and coexist with the protocols listed above: SSH-TRANS, SSH-AUTH and SSH-CONNECT.
- SSH and SFTP provide server functionality only; client functionality is not provided.

SSH Server Functionality

The following summarizes the SSH functions and constraints.

- The SSH server supports up to three (3) concurrent connections.
- The SSH server listens for connections on a single TCP port.
- The port can be set to which the SSH server listens for connections.
- When a connection is accepted, it is handled first by the SSH-TRANS subsystem.

- You cannot set the SSH server to run on a port in use by another TCP service, such as Telnet or HTTP.
- The SSH server can be enabled or disabled.
- Current SSH client connections are not dropped when the SSH port is changed or the SSH server is stopped.

SFTP

SFTP provides secure file transfer between an SFTP client and the BSGX4e. This enables the secure upload of binary applications to the BSGX4e file system.

Users with administrator rights are allowed to upload and download public key files through SFTP. The file name of a user's public key is `/cf0sys/id_<username>.pub`.

If the SSH client requests the SFTP service, the SFTP server gives the user the following file access permissions:

- Full read-write access to the `/cf0usr` file system volume.
- For users with full administrator rights, access to the `/cf0sys` volume.

Authentication

After a secure method of data transport between an SSH client and the SSH server is established, and the server identifies itself through its host keys, a client can attempt authentication.

The SSH server supports password, keyboard-interactive, and public-key authentication. The SSH server configuration determines which authentication methods it offers to clients:

- **Password Authentication**
  Password authentication is requested on the client side and then sent to the SSH server. The user is prompted with the following:
  - `User:`
  - `Password:`
- **Keyboard-Interactive Authentication**
  Using keyboard-interactive authentication, the following prompts appear:
  - `User:`
  - `Password:`
- **Public Key Authentication**
  Public key authentication requires that the user upload a public key file from the SSH client to the BSGX4e. Users with administrator rights can upload and download public key files through SFTP. The file name of a user's public key is: `/cf0sys/id_<username>.pub`.

After the user is authenticated, the SSH client requests the desired SSH service: SSH secure remote log on or SFTP. You can configure which SSH services are offered. See "SSH Server" (page 36).

Host Keys

When an SSH client connects, the SSH server negotiates a method to securely encrypt the data transport between itself and the SSH client (cipher selection) and to identify itself to the client (host key exchange).

Should a security breach occur, such as accidental disclosure of the private host key, new host keys can be generated through the CLI or the Web UI.

Users with administrator rights also have read/write permissions to the public and private host keys through SFTP. The file names of the public and private host keys, known only to the SFTP server, are respectively `/cf0sys/ssh/dsakey.pub` and `/dsakey.priv`.

The SSH server uses this set of host keys to identify itself when an SSH client connects. See "SSH-TRANS" (page 404).

Remote Log on

Remote log on can be provided with SSH or SFTP service (see "SSH Server Functionality" (page 401)).

When an SSH client requests SSH secure remote log on, the session begins with the CLI command prompt. The `User:` and `Password:` prompts do not appear as the user has been authenticated through the SSH server.

When an SSH client requests SFTP service, the SFTP server provides the user with the appropriate user access:

- All users are granted full read-write access to the `/cf0usr` file system volume.
- Users with full administration rights also have access to the `/cf0sys` volume.

Service Functions

The following sections describe the service functions of SSH and SFTP.

SSH Service

User authorization is processed by the SSH-AUTH subsystem; the `User:` and `Password:` prompts do not appear. Full access to CLI is provided to the user; the command prompt is displayed immediately.

The SSH service can be enabled or disabled. When SSH service is enabled, authenticated SSH clients are allowed to begin an SSH session. When SSH service is disabled, existing SSH sessions are not affected.

SSH service is compatible with recent versions of the OpenSSH SSH client and the PuTTY SSH client.

SFTP Service

SFTP service can be enabled or disabled. When SFTP service is enabled, authenticated SFTP clients are allowed to begin an SFTP session. When the SFTP service is disabled, existing SFTP sessions are not affected.

At a minimum, SFTP is compatible with recent versions of the OpenSSH SFTP client and the WinSCP SFTP client.

Depending on how file access permissions are set, the following actions are available:

- Navigate the file system
- Create and remove files
- Create and remove directories

The SFTP service provides the means for uploading application binaries.

The file access permissions are defined as follows: all users have full read-write access to the /cf0usr file system volume, users with full administrator rights also have access to the /cf0sys volume.

When an SFTP client connects, the initial working directory is `/cf0usr`.

SSH System Architecture

The SSH server consists of three subsystems: SSH-TRANS, SSH-AUTH, and SSH-CONN.

SSH-TRANS

The SSH-TRANS subsystem provides a choice of ciphers to encrypt data transport between the SSH client and the SSH server. The subsystem uses a set of host keys to identify the SSH server.

The SSH-TRANS subsystem offers ciphers to SSH clients during algorithm negotiation. The SSH-TRANS subsystem supports the following ciphers:

- aes256-cbc
- aes-192-cbc
- aes-128-cbc
- rinjdael256-cbc
- rinjdael192-cbc
- rinjdael128-cbc
- blowfish-128-cbc
- 3des-192-cbc
- arcfour-128

During key exchange, the SSH-TRANS subsystem identifies the SSH server by using the current host keys in memory. The SSH-TRANS subsystem stores one set of 640-bit DSA host keys in memory. A randomly seeded algorithm generates the first set of host keys the first time that the BSGX4e is booted.

To generate new host keys, existing host keys can be deleted. Host key generation can take up to 30 minutes. The host keys are stored on the file system: `/cf0sys/ssh/dsakey.pub` and `/cf0sys/ssh/dsakey.prv`.

SSH-AUTH

The SSH-AUTH layer provides three authentication methods:

- Password authentication
- Keyboard-interactive authentication
- Public key authentication

SSH-CONNECTION

The SSH-CONNECTION layer provides the SSH secure remote log on service and the SFTP secure file transfer service. It provides these services only to users who successfully authenticate with the SSH-AUTH layer:

- The SSH secure remote log on service provides full access to the CLI.
- The SFTP service provides access to the DOS FS file system, and upgrade functionality.

D

TCPDUMP EXPRESSIONS

This appendix provides information about *expression* options for the **tcpdump** command. The command is described in "TCPdump Command" (page 352).

Introduction

You can specify expression on the debug command **tcpdump**. An expression selects which packets are dumped. If no expression is given, all packets on the net are dumped. Otherwise, only packets for which expression is *true* are dumped.

Expressions

The expression consists of one or more primitives. Primitives usually consist of an identifier (name or number) preceded by one or more qualifiers. Three types of qualifiers exist:

- Type qualifiers

  Type indicates the type of to which object the identifier (name or number) refers. The available types are `host`, `net` and `port`. Example: `host foo`, `net 128.3`, `port 20`. If no type qualifier exists, `host` is assumed.

- Dir qualifiers

  Specifies a particular transfer direction to and/or from id. The available directions are `src`, `dst`, `src or dst`, **and** `src and dst`. Example: `src foo`, `dst net 128.3`, `src`, or `dst port ftp-data`. If no dir qualifier exists, `src` or `dst` is assumed.

- Proto qualifier

  Restricts the match to a particular protocol. The available protos are `ether`, `ip`, `arp`, `rarp`, `tcp` and `udp`. Example: ether src foo, arp net 128.3, tcp port 21. If no proto qualifier exists, all protocols consistent with the type are assumed. Example: `src foo` indicates (`ip`, `arp`, or `rarp`) `src foo` (except the latter, `foo`, is not legal syntax), `net bar` indicates (`ip`, `arp`, or `rarp`) `net bar` and `port 53` indicates (`tcp` or `udp`) `port 53`.

Primitives

In addition to expressions, there are *`primitive`* keywords that do not follow the pattern: `gateway`, `broadcast`, `less`, `greater` and mathematical expressions.

- More complex filter expressions are built up by combing primitives with the following operations: and, or not. Example: `host foo and not port ftp and not port ftp-data`.
- Identical qualifier lists can be omitted. Example: entering `tcp dst port ftp or ftp-data or domain` is the same as entering `tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain.`

The following is a description of the allowed primitives:

`dst host host`
True if the IPv4 destination field of the packet is `host`, which must be an IP address.

`src host host`
True if the IPv4 source field of the packet is `host`.

`host host`
True if either the IPv4 source or destination of the packet is `host`.

`ether dst ehost`
True if the ethernet destination address is `ehost`.

`ether src ehost`
True if the ethernet source address is `ehost`.

`ether host ehost`
True if either the ethernet source or destination address is `ehost`.

`gateway host`
True if the packet used host as a `gateway`. For example, when the ethernet source or destination address is host but neither the IP source nor the IP destination is host.

`dst net net`
True if the IPv4 destination address of the packet has a network number of `net`.

`src net net`
True if the IPv4 source address of the packet has a network number of `net`.

`net net`
True if either the IPv4 source or destination address of the packet has a network number of `net`.

`net net mask netmask`
True if the IP address matches `net` with the specific `netmask`.

`net net/len`
True if the IPv4 address matches `net` with a netmask `len` bits wide.

`dst port port`
True if the packet is ip/tcp or ip/udp and has a destination port value of `port`.

`src port port`

True if the packet has a source port value of `port`.

`port port`
True if either the source or destination port of the packet is `port`.

`less length`
True if the packet has a length less than or equal to `length`.

`greater length`
True if the packet has a length greater than or equal to `length`.

`ip proto protocol`
True if the packet is an IP packet of protocol type `protocol`. Protocol can be a number or one of the following names—icmp, udp, or tcp. Note that the identifiers tcp, udp, and icmp are also keywords and must be escaped through backslash (\).

`ip protochain protocol`
True if the packet is an IPv4 packet and contains protocol of protocol type `protocol`.

`ether broadcast`
True if the packet is an ethernet broadcast packet. The ether keyword is optional.

`ip broadcast`
True if the packet is an IPv4 broadcast packet.

`ether multicast`
True if the packet is an ethernet multicast packet. The ether keyword is optional.

`ip multicast`
True if the packet is an IP multicast packet.

`ether proto protocol`
True if the packet is of ether type `protocol`. Protocol can be a number or one of the following names—`ip`, `arp`, `rarp`, or `stp`. Note these identifiers are also keywords and must be escaped through backslash (\).

`ifname interface`
True if the packet is logged as coming from the specified `interface`.

`on interface`
Synonymous with the ifname modifier.

`ip, arp, rarp, stp`
Abbreviations for `ether proto p` where p is one of the above protocols.

`vlan [vlan_id]`
True if the packet is an IEEE 802.1Q VLAN packet. If [`vlan_id`] is specified, the only true packet has the specified `vlan_id`.

`tcp, udp, icmp`

Abbreviations for `ip proto p` where p is one of the above protocols.

`expr relop expr`

True if the relation holds, where `relop` is one of >, <, >=, <=, =, !=, and `expr` is an arithmetic expression composed of integer constants, the normal binary operators [`+, -, *, /, &, |, <<, >>`], a length operator, and special packet data accessors. To access data inside the packet, use the following syntax: `proto [expr: size]`.
`Proto` is one of `ether, ip, arp, rarp, tcp, udp, or icmp`, and indicates the protocol layer for the index operation. The byte offset, relative to the indicated protocol layer, is given by `expr`. `Size` is optional and indicates the number of bytes in the field of interest; it can be either one, two, or four, and defaults to one. The length operator, indicated by the keyword `len`, gives the length of the packet.

Some offsets and field values can be expressed as names rather than as numeric values.

- The following protocol header field offsets are available: icmptype (ICMP type field), icmpcode (ICMP code field), and tcpflags (TCP flags field).
- The following ICMP type field values are available: icmp-echoreply, icmp-unreach, icmp-sourcequench, icmp-redirect, icmp-echo, icmp-routeradvert, icmp-routersolicit, icmp-timxceed, icmp-paramprob, icmp-tstamp, icmp-tstampreply, icmp-ireq, icmp-ireqreply, icmp-maskreq, icmp-maskreply.
- The following TCP flags field values are available: `tcp-fin, tcp-syn, tcp-rst, tcp-push, tcp-ack, tcp-urg.`

Primitives can be combined as follows:

- A parenthesized group of primitives and operators.
- Negation (`!' or `not').
- Concatenation (`&&' or `and').
- Alternation (`||' or `or').

Negation has highest precedence. Alternation and concatenation have equal precedence, and associate from left to right.

E
STANDARDS COMPLIANCE

This appendix lists the standards to which the BSGX4e device complies.

Data Standards

Switching

Table 122. Switching

Standard	Description
IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.
IEEE 802.3x	IEEE 802.3 Full Duplex Operation.
IEEE 802.1D MAC	Media Access Control (MAC) Bridges.
IEEE 802.1Q	Virtual Bridged Local Area Networks.

Routing

Table 123. Routing

Protocol	IETF RFC	Description
IP	791	Internet Protocol
UDP	768	User Datagram Protocol
TCP	793	Transmission Control Protocol
ICMP	777	Internet Control Message Protocol
RIP	1058	Routing Information Protocol version 1
RIPv2	2453	RIP version 2

Security

Table 124. NAT Security

IETF RFC	Description
1631	The IP Network Address Translator (NAT)
2663	IP Network Address Translator (NAT) Terminology and Considerations
2767	Address Translation - Protocol Translation (NAT-PT)
3022	Traditional IP Network Address Translator (Traditional NAT).

Table 125. IKE Security

IETF RFC	Description
2407	The Internet IP Security Domain of Interpretation for ISAKMP
2408	Internet Security Association and Key Management Protocol (ISAKMP)
2409	The Internet Key Exchange (IKE)

Table 126. IPsec Security

IETF RFC	Description
4303	IP Encapsulating Security Payload (ESP)
4305	Cryptographic Algorithms for ESP & AH
4308	Cryptographic Suites for IPsec (definition of VPN-A proposal)

Quality of Service

Table 127. Quality of Service

IETF RFC	Description
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
2475	An Architecture for Differentiated Service
3246	An Expedited Forwarding PHB (Per-Hop Behavior)

Services

Table 128. Services

Service	IETF RFC	Description
Telnet	854	Telnet Protocol Specification
FTP	959	File Transfer Protocol
DNS	1034	Domain names—concepts and facilities
DNS	1035	Domain names—implementation and specification
NTP	1305	Network Time Protocol (Version 3) Specification, Implementation
TFTP	1350	The TFTP protocol (Revision 2)
HTTP	1945	Hypertext Transfer Protocol, HTTP/1.0
SNTP	2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6, and OSI
DHCP	2131	Dynamic Host Configuration Protocol
DHCP	2132	DHCP Options and BOOTP Vendor Extensions
RADIUS	2138	Remote Authentication Dial In User Service (RADIUS)
	2246	TSL Protocol Version 1.0
ISKMP	2459	Internet Public Key Infrastructure
DNS	2782	A DNS RR for specifying the location of services (DNS SRV)
SSH	4250	The Secure Shell (SSH) Protocol Assigned Numbers
SSH	4251	The Secure Shell (SSH) Protocol Architecture
SSH	4252	The Secure Shell (SSH) Authentication Protocol
SSH	4253	The Secure Shell (SSH) Transport Layer Protocol
SSH	4254	The Secure Shell (SSH) Connection Protocol
SSH	4256	Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)
SSH	4344	The Secure Shell (SSH) Transport Layer Encryption Modes

Monitoring

Table 129. Monitoring

Service	IETF RFC	Description
TCPdump	1155	Structure and Identification of Management Information for TCP/IP-based Internets
SNMP	1157	Simple Network Management Protocol (SNMP)
SNMP	1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II

Table 129. Monitoring (continued)

Service	IETF RFC	Description
SNMP	1215	Convention for defining traps for use with the SNMP
SNMP	1901	Introduction to Community-based SNMPv2
SNMP	1902	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
SNMP	1903	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
SNMP	1904	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
SNMP	1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
SNMP	1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
NetFlow	3954	Cisco Systems NetFlow Services Export Version 9

Voice Standards

SIP Session Controller

Table 130. SIP Session Controller

Standard	Description
IETF RFC 2327	SDP: Session Description Protocol
IETF RFC 2806	URLs for Telephone Calls
IETF RFC 2976	The SIP INFO Method
IETF RFC 3261	SIP: Session Initiation Protocol (except TCP)
IETF RFC 3262	Reliability of Provisional Responses in Session Initiation Protocol (SIP)
IETF RFC 3263	Session Initiation Protocol (SIP) - Locating SIP Servers
IETF RFC 3264	An Offer/Answer Model with Session Description Protocol (SDP)
IETF RFC 3265	Session Initiation Protocol (SIP) - Specific Event Notification
IETF RFC 3515	The Session Initiation Protocol (SIP) - Refer Method
IETF RFC 3550	RTP: A Transport Protocol for Real-Time Applications
IETF RFC 3725	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
IETF RFC 3842	A Message Summary and Message Waiting Indication Event Package
IETF RFC 3891	The Session Initiation Protocol (SIP) “Replaces” Header

Table 130. SIP Session Controller (continued)

Standard	Description
IETF RFC 3892	The Session Initiation Protocol (SIP) Referred-By Mechanism
IETF RFC 3966	The tel Uniform Resource Identifier (URI) for Telephone Numbers
IETF RFC 4028	Session Timers in the Session Initiation Protocol (SIP)
	IETF draft-ietf-sipping-torture-tests-00: SIP torture tests
ITU T.38	Procedures for Real-time Group 3 facsimile communication over IP networks
ITU P.800	Mean Opinion Score (MOS)
ITU P.861	Perceptual Speech Quality Measure (PSQM)

MGCP Session Controller

Table 131. MGCP Session Controller

Standard	Description
IETF RFC 3435	Media Gateway Control Protocol (MGCP) Version 1.0
IETF RFC 2327	Session Description Protocol
IETF RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
IETF RFC 3149	Media Gateway Control Protocol (MGCP) Business Phone Packages
IETF RFC 3660	Basic Media Gateway Control Protocol (MGCP) Packages
IETF RFC 3661	Media Gateway Control Protocol (MGCP) Return Code Usage
IETF RFC 3550	RTP: A Transport Protocol for Real-Time Applications
ITU T.38	Procedures for Real-time Group 3 facsimile communication over IP networks
ITU P.800	Mean Opinion Score (MOS)
ITU P.861	Perceptual Speech Quality Measure (PSQM)

SIP User Agent (Integrated Gateway)

Table 132. SIP User Agent

Standard	Description
IETF RFC 2327	Session Description Protocol
IETF RFC 2833	RTP Payload for DTMF Digits, Telephone Tones, and Telephony Signals
IETF RFC 2916	E.164 number and DNS
IETF RFC 3261	Session Initiation Protocol (SIP) (except TCP)

Table 132. SIP User Agent (continued)

Standard	Description
IETF RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
IETF RFC 3263	Session Initiation Protocol (SIP) - Locating SIP Servers
IETF RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
IETF RFC 3265	Session Initiation Protocol (SIP) - Specific Event Notification
IETF RFC 3515	The Session Initiation Protocol (SIP) - Refer Method
IETF RFC 3550	RTP: A Transport Protocol for Real-Time Applications
IETF RFC 3725	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
IETF RFC 3842	A Message Summary and Message Waiting Indication Event Package
IETF RFC 4028	Session Timers in the Session Initiation Protocol (SIP)
	IETF draft-ietf-sipping-mwi-04.txt: A Message Summary and Message Waiting Indication Event Package for SIP
	IETF draft-ietf-sipping-realtimefax-01.txt: SIP Support for Real-time Fax
ITU G.711 aLaw/uLaw	Pulse code modulation (PCM) of voice frequencies
ITU G.729 A/B	Coding of speech at 8 kbit/s using conjugate
ITU G.168	Echo Cancellation
ITU T.30	Procedures for document facsimile transmission in the general switched telephone network

MGCP User Agent (Integrated Gateway)

Table 133. MGCP User Agent

Standard	Description
IETF RFC 3435	Media Gateway Control Protocol (MGCP) Version 1.0
IETF RFC 2327	Session Description Protocol
IETF RFC 3264	An Offer/Answer Model with the Session Description Protocol (SDP)
IETF RFC 3149	Media Gateway Control Protocol (MGCP) Business Phone Packages
IETF RFC 3660	Basic Media Gateway Control Protocol (MGCP) Packages
IETF RFC 3661	Media Gateway Control Protocol (MGCP) Return Code Usage
IETF RFC 3550	RTP: A Transport Protocol for Real-Time Applications
IETF RFC 2833	RTP Payload for DTMF Digits, Telephone Tones, and Telephony Signals

Table 133. MGCP User Agent (continued)

Standard	Description
ITU G.711 aLaw/uLaw	Pulse code modulation (PCM) of voice frequencies
ITU G.729 A/B	Coding of speech at 8 kbit/s using conjugate
ITU G.168	Echo Cancellation
ITU T.30	Procedures for document facsimile transmission in the general switched telephone network

F
RULE COMPLIANCE

This appendix lists telecommunication rule compliance information for the BSGX4e device.

FCC Compliance (U.S.)

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference
- This device must accept any interference received, including interference that can cause undesired operation

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, can cause harmful interference to radio communications. However, no guarantee exists that interference will not occur in a particular installation. If this device does harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Telecom Statement

This device complies with Part 68 of the FCC rules and requirements adopted by the ACTA. On the bottom of this device is a label that includes, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, you must provide this number to the telephone company.

A plug or jack used to connect this device to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. The BSGX4e unit is designed to be connected to a compatible modular jack that is also compliant. For details, see the installation instructions provided in the installation manual.

- The Universal Service Order Codes (USOC) for this device (BSGX4e) are 9.0F.

- The Facility Interface Codes (FIC) and the Service Order Codes (SOC) for this device (BSGX4e) are 02LS2.
- The REN# for this device (BSGX4e) is 0.0.

  The REN is used to determine the number of devices that can be connected to a telephone line. Excessive RENs on a telephone line can result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the total RENs, contact the local telephone company. The REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3).

If this device (BSGX4e) causes harm to the telephone network, the telephone company notifies you in advance that temporary discontinuance of service can be required. But if advance notice is not practical, the telephone company notifies the customer as soon as possible. Also, you are advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company can make changes in its facilities, equipment, operations, or procedures that can affect the operation of the device. If this happens, the telephone company provides advance notice so you can make necessary modifications to maintain uninterrupted service.

If the device causes harm to the telephone network, the telephone company can request that you disconnect the device until the problem is resolved. For any detailed repair and troubleshooting information, contact "How to get help" (page 26).

Connecting the party line service is subject to tariffs. For information, contact the state public utility commission, public service commission, or corporation commission.

If your home or office has specially-wired alarm equipment connected to the telephone line, ensure the installation of this device. (The BSGX4e does not disable your alarm equipment. If you have questions about what disables alarm equipment, consult your telephone company or a qualified installer.)

WARNING: Any changes or modifications to this product not expressly approved by the manufacturer could void any assurance of safety or performance and could result in violation of Part 15 of the FCC Rules.

Declaration of Conformity

We, the responsible party, declare that the product conforms to the following standards:

- FCC part15, subpart B, class B

  Manufacturer name: Accton Corporation
  Product name: Business Gateway
  Model: BSGX4e

Equipment Attachment Regulations (Canada)

NOTICE: The industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction. Before installing this equipment, users should ensure that is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection.

The customer should be aware that compliance with the above conditions can not prevent degradation of service in some situations. Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs of alternations made by the user, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution can be particularly important in rural areas.

Canadian Department of Communications Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

The Class B Detail apparatus complies with Canadian ICES-003.

Supplementary Information

This device is in conformance with the following standards:

- FCC part15 class B
- UL 60950
- CAN/CSA-C22.2 No.60950

G
COPYRIGHT INFORMATION

This appendix lists important copyright Information and acknowledgments.

GoAhead Software, Inc.

Copyright © 2005 GoAhead Software, Inc. All Rights Reserved.

The Regents of the University of California

Portions of this product are:

Copyright © 1987, 1988, 1989, 1990, 1991, 1992, 1994, 1995, 1996, 1997 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement:

"This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.'"

Neither the name of the University nor the names of its contributors can be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS'" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Notables Foundation, Inc.

Portions of this product are:

Copyright © 1998 The NetBSD Foundation, Inc. All rights reserved.

This code is derived from software contributed to the NetBSD Foundation by Christos Zoulas.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. **Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.**

2. **Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.**

3. **All advertising materials mentioning features or use of this software must display the following acknowledgement:**

   This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

4. **Neither the name of The NetBSD Foundation nor the names of its contributors can be used to endorse or promote products derived from this software without specific prior written permission.**

THIS SOFTWARE IS PROVIDED BY THE NetBSD Foundation, INC. AND CONTRIBUTORS “AS IS" AND ANY TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Maxim Sobolev

Copyright © 2003 Maxim Sobolev. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Lars Feneberg

Copyright © 1995,1996,1997,1998 Lars Fenneberg

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg.

Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

Livingston Enterprises, Inc.

Copyright © 1992 Livingston Enterprises, Inc.

Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc.

LIVINGSTON ENTERPRISES, INC. MAKES NO REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. IT IS PROVIDED “AS IS” WITHOUT EXPRESS OR IMPLIED WARRANTY.

The Regents of the University of Michigan and Merit Network, Inc.

Copyright © 1992, 1993, 1994, 1995 The Regents of the University of Michigan and Merit Network, Inc. All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation.

THIS SOFTWARE IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE.

The Regents of the University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

RSA Data Security, Inc.

Copyright © 1991-1992, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Damien Miller

Portions of this product are:

Copyright © 2002 Damien Miller All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. **Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.**
2. **Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.**

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Neil Provos

Portions of this product are:

Copyright © 2002 Neil Provos. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. **Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.**

2. **Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.**

   THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Kevin Steves

Portions of this product are:

Copyright © 2001 Kevin Steves. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. **Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.**

2. **Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.**

   THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Todd C. Miller

Portions of this product are:

Copyright © 1998 Todd C. Miller

Permission to use, copy, modify and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THIS SOFTWARE IS PROVIDED ``AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARDS TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

H
GLOSSARY

3PCC	3rd Party Call Control.
ALG	Application Layer Gateway.
ARL	Address Resolution Logic.
CAC	Call Admission Control.
CAS	Channel Associated Signaling.
CDP	Cisco Discovery Protocol.
CLI	Command Line Interface.
CO	Central Office; refers to the connection to the PSTN.
DHCP	Dynamic Host Configuration Protocol; used to assign and manage IP addresses for a network.
DLCI	Data Link Connection Identifier: defines the destination of packet. Used by PVC.
DNS	Domain Name Server.
EAC	Endpoint Access Control.
EP	Endpoint; port of a gateway or a phone.
ESP	Encapsulated Security Payload; protocol that defines the encrypted packets sent through a VPN tunnel.
Failover	Backup system used to continue operations if the main device goes down. During a power interruption, an analog telephone connected to the device can place emergency calls.
FIFO	First-In First-Out. A queued method for storing and retrieving data.
FQDN	Fully Qualified Domain Name, consisting of host and domains. For example, *www.yahoo.com*: the host is *www*, the second-level domain is *yahoo*, and the top-level domain is *com*.
FXO	Foreign Exchange Office. Provides interface on a VoIP device to connect to phones, faxes, and CO ports on a PBX or key telephone systems.

FXS	Foreign Exchange Station. Device interface that connects to an analog device such as a telephone or fax machine.
GoS™	Guarantee of Service.
IDS	Intrusion Detection System; defends the device from attacks arriving from the WAN.
IKE	Internet Key Exchange; protocol used to negotiate the initial security association between gateways of a VPN tunnel.
IPsec	Internet Protocol Security; protocol used to secure VPNs across an IP network.
ISDN	Integrated Services Digital Network.
LAN	Local Area Network.
MAC	Meda Access Control. A MAC address is a hardware address that uniquely identifies each network device.
MGC	Media Gateway Controller.
MGCP	Media Gateway Control Protocol.
NAT	Network Address Translation. Also known as Network Address Translator.
NTP	Network Time Protocol. See SNTP.
PCM	Pulse Code Modulation.
POTS	Plain Old Telephone Service.
PRI	Primary Rate Interface.
PSTN	Public Switched Telephone Network.
PVC	Permanent Virtual Circuit.
RTCP	Real Time Transport Control Protocol (or RTP Control Protocol).
RTP	Real-Time Transfer Protocol.
SA	Security Association; used by IKE and IPsec to determine how data is encrypted, decrypted, and authenticated by the secure gateways.
SC	Session Controller.
SFC	Stateful Flow Controller.
SFTP	Simple File Transfer Protocol; can be used to transfer software upgrades to the device.
SHA	Strong password HAshing.
SIP	Session Initiation Protocol.

SIP UA	SIP User Agent.
SLIC	Subscriber Line Interface Circuit.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet.
SRV	DNS method/messages for location of services.
Stateful	Maintains the last-known or current status of an application.
TDM	Time Division Multiplex.
TFTP	Trivial File Transfer Protocol.
UDP	User Datagram Protocol. A connectionless protocol that allows direct delivery and receipt of datagrams, without acknowledgements or guarantee of delivery.
VoIP	Voice over Internet Protocol.
VPM	Voice Processing Module.
VPN	Virtual Private Network; a means for secure communication across an insecure network, such as the Internet.
WAN	Wide Area Network.

INDEX

A

AC impedance register for FxO port 260
Access Control List 232
access method limitation 58
access rights
  inheritance 62
access rights settings 61
account configuration 61
acknowledgments 423
ACL. See Access Control List
Acrobat Reader 399
active user listing 60
address forwarding 138
  NAT 134
Address Resolution Logic. See ARL
Address Resolution Protocol. See ARP
administrator 61
alarms
  log entries 252
  statistics 252
ALG
  configuration 140
all keyword 85
analog device
  MGCP gateway 211
  SIP gateway 265
  telephone features
    MGCP 211
    SIP 265
analyser, voice quality 247
anomaly protection 141
Application Layer Gateway. See ALG
application software images 362
  changing default 368
area code 258
ARL
  configuration 104
  QoS 104
  remove entry 106
  table flush 106
  table listing 105
ARP
  attack protection 141
  configuration 122
  definition 121

entry configuration 122
flood protection 144
table
flushing 123
listing 122
traffic protection 123, 191
attack protection, IDS 140
audio quality group 230
audit logging 324
AUEP requests 211
authentication
ACL endpoint 232
IPsec 153
RADIUS client 68, 71
Radius client 68, 71
SIP account 281
SSH 36
TACACS+ client 74
user password 62, 65
authenticationfail 347
authority
debug commands 88
maintenance commands 86
settings 61
user management 57
autorun commands 80

B

back pressure 98
backup call servers
MGCP 212
SIP 266
backup phone service 255
BE. See best effort
best effort
class 183
default quality group 188
link capacity 187
policing 185
blacklist
MGCP call server 212
SIP call server 266
boolean parameters 84
bootloader selection 366
burst setting 184

C

CAC. See Call Admission Control
cache
DNS relays 314
TFTP files 318

Call Admission Control 236
call limit
MGCP 217
SIP 273
call progress tone configuration 241
call quality 247
call records 231
call history 254
calls in progress 253
MGCP 220
SIP 276
call server
MGCP 212
call statistics 231
MGCP 219
CAR policing 184
CDP 234
flood protection 144
central office prefix 258
change password 58, 59
Cisco Discovery Protocol 234
Cisco SIP phone 7960 288
CLI
debug commands
online help 81
interactive mode 82
keyword
all 85
no 84
maintenance commands
online help 81
online help 81
specific 81
parameter values 84
syntax 83
client
DNS 50
CO telephone line 256
CODECs
MGCP gateway 223
SIP gateway 280
statistics 249
coldstart 347
command entry 77
autorun 80
customizing 78
Command Line Interface. See CLI
command prefixes 83
command prompt 77
changing 79
interactive mode 83
pending changes 80
command syntax 83

debug commands 88
keywords
all 85
no 84
maintenance commands 86
parameter values 84
committed access rate. See CAR policing.
community configuration 348
configuration
as shipped 53
default 52
dump 80
listing example 374
restoring after upgrade 369
save 79
saving before upgrade 363
configuration examples
VPN 163
configuration listing 80
configure
static route delete 126
static routing 124
web server 42
connecting to the unit 32
Connection Protocol 401
connection timeout 133
connections to device 34
console
logging destination 327
console port lockout 58
contention 181
copyright information 423
CoS tag values 189
country code setting 239
CPU usage 323
CSR 41
upload 42

D

debug
command authority 88
command listing 88
command syntax 88
commands 88
online help 81
message severity 326
monitoring tools 339
system exceptions 321
tcpdump 352
default configuration 52
default route 125
denial of service attack 141

device features 30
device name change 239
DH group 159
DHCP
  eth0 interface 92
  flood protection 145
  leases 312
  option 42 315
  option 6 313
  option 66 316
  relay 312
  server 309
Diffie-Hellman group 159
DiffServ/ToS tags
  layer 2 QoS 109
digit maps 211
direct media connections 229
directory commands 359
DNS
  client 50
  flood protection 145
  relay 313
  relay cache 314
  session listing 314
  SRV 266
documentation feedback 2
downgraded packets 187
dropped packets 187
DSA host keys 36
  regenerate 37
DSP gain settings
  FxO port 259
  FxS port 243
DSP tone configuration 241
DSP tone settings 241
DTMF
  SIP gateway 225, 281
dump
  example 374
  show configuration 80
duplex mode 97
  WAN port 92

E

electrical status
  FxS ports 244
emergency call number 258
encryption, IPsec 153
endpoint
  authentication 232
  MGCP
    timeout parameter 217

MGCP configuration 227
MGCP ID 224
phone numbers 256
SIP registration expiration 277
SIP registration list 276
timer
MGCP 221
SIP 277
Endpoint Status Handling. See ESH
ESH
MGCP 220
SIP 277
ESP
flood protection 144
IPsec proposals 160
eth0
statistics 94
eth0 interface 92
eth1 interface
configuration 102
Ethernet interface
eth0 92
WAN 92
Ethernet statistics 331
exception listing 321
exit
ending a session 78
external authentication
TACACS+ client 74

F

failed login attempts 58
failover
MGCP call server 212
SIP call server 266
fax pass-through
MGCP gateway 225
SIP gateway 280
feature list 30
feedback, documentation 2
file cache, TFTP 318
file commands 360
file system 359
management 360
navigation 359
firewall
ALG for FTP and TFTP 140
gateways for FTP and TFTP 140
log entries 132
rules 130
security policies 130
flash memory 359

flood protection 143
flood thresholds 145
flow control 98
  disabled for layer 2 QoS 98
  layer 2 QoS constraints 107
foreign voltages test 245
formatting memory commands 361
forwarding
  NAT
    by address 138
    by port 137
forwarding database
  ARL 104
fragment overlap anomaly 142
fragment overrun anomaly 142
FTP
  ALG support 140
  connection timeout 133
  download files 318
FXO port 31
FxO port
  call routing 256
FXS port 31
FxS port
  configuration 238
  electrical status 244
  tone configuration 241

G

gain settings
  FxO port 259
  FxS port 243
gateway
  MGCP 211
    configuration 222
  SIP 265
    configuration 280
GoS 181
  link
    configuration 186
    listing 186
  quality group
    listing 190
  security policies 191
    listing 193
  statistics
    cumulative 193
    instantaneous 195
  traffic flow assignment 190
GR-909 metallic loop tests 245
Guarantee of Service. See GoS

H
hardware information 322
hazardous voltage test 245
help
  CLI commands 81
  debug commands 88
  maintenance commands 86
hook flash 211
host keys, SSH server 36
HTTP
  web server access 38
HTTP connection timeout 133
HTTPS
  web server access 38
hybrid filters for FxO port 261

I
IAD 211
ICMP
  attack protection 141
  flood protection 143
  scan protection 146
  statistics 333
IDS
  anomaly protection 141
  configuration 140
  flood protection 143
  log 150
  log entries 150
  scan protection 146
  spoof protection 147
  statistics 149
IEEE 802.1p tags
  layer 2 QoS 108
IKE 154
  flood protection 145
  negotiation port 156
impedance settings
  FxO port 260
  FxS port 243
inbound mapping 134
inbound servers
  SIP 266
in-contract region 184, 185
initial configuration 53
integrated access device 211
Integrated Gateway 30
  MGCP 211, 222
  SIP 278
interactive command entry 82
interface

NAT enabling 135
VLAN 114
Internet Key Exchange 154
Internet Protocol. See IP
Intrusion Detection Service. See IDS
IP
address range specification 84
attack protection 141
IP address
VLAN 114
IP interface
eth1 102
IP interface statistics 331
IP routing
configuration 124
definition 121
IP routing stack statistics 331
IP ToS tag values
written by GoS 189
IPsec 154

J

jitter buffer
settings 240
simulation 247
statistics 240

K

keep alive functions
MGCP 210
parameter 217
key
CSR 41
DSA host 36
IKE preshared 156
regeneration for SSH 37
SSL 40
upload public key for SSH client 38
keyword
all 85
no 84

L

LAN
VLAN 111
LAN port
listing 99
mirroring 339
statistics 100
LAN switch 97
configuration 97

layer 2 QoS 106
packet classification 107
port mapping 108
priority queues 107
queuing mechanisms 107
scheduling methods 107
tag mapping
DiffServ/ToS 109
tag mappng
IEEE 802.1p 108
LCR
connections 262
gateway 257
status 262
leases, DHCP 312
lifeline 30
line fault testing 245
line impedance settings
FxO port 260
FxS port 243
line status
MGCP gateway 226
line width, command entry 79
linkdown 347
linkup 347
listing
current configuration 374
directory contents 360
file contents 360
partition formatting 361
lockout of console port 58
logging
audit 324
call quality alarms 252
destination map 327
destinations 327
IDS attack detection 150
IDS attacks 150
login attempts 58
map 327
message levels 326
message severities 326
modules 325
packets denied by firewall 132
Radius activity 71, 74
server specification 329
server statistics 330
system modules 325
user management 58
logging file 327
login attempts 58
logo display 309
logout 78

M

MAC address
- ARL mapping 104
- device interfaces 323
- priority queues 104

main mode IKE negotiation 156
maintenance commands 86
- authority 86
- listing 86
- online help 81, 86
- syntax 86

Man-in-the-Middle attacks 144
map
- ARL 104
- MAC addresses to LAN ports 104

MBR (see Media Bridge) 229
Media Bridge 229
media connections
- limit 230
- settings 229

Media Gateway Control Protocol. See MGCP
Media Gateway Controller 212
media stream
- status
  - MGCP gateway 226
  - SIP gateway 283

memory
- size 323

message severities 325
MGC 212
MGCP 209
- Access Control List 232
- Call Admission Control 236
- call records 220, 232
- call server 212
  - profile 213
  - status 214
- endpoint registration 220
- flood protection 145
- FXS port configuration 238
- gateway 211
  - configuration 222
  - status 226
- keep-alive functions 210
- Media Bridge 229
- session controller 210
  - status 218
- signaling statistics 218
- user agent 211

MGCP Signaling Proxy. See MSP
MIBs 347
MII port 97

mii0
WAN port 91
mirroring traffic 339
mob.cfg.cpy file
restoring configuration 369
saving configuration 365
modem pass-through
MGCP gateway 225
SIP gateway 280
module logging 325
monitoring
information displays 321
protocol traffic 340
tools 339
voice quality 247
MOS scores
calculation 247
detail 251
summary 250
MSP 216
MTU
eth0 interface 92
eth1 interface 102
multicasting support 126
multi-line support 282
multi-service QoS 31

N

NAPT 134
NAS 69, 72
TACACS+ 74
NAT
address forwarding 134, 138
configuration 134
interface 135
status 135
overload 134
policies 135
listing 139
port forwarding 134, 137
public addresses 136
reverse 134
standard 134
static 134
static forwarding 138
neighbor summary, CDP 235
Netflow exporter 343
Network Access Server 69, 72
TACACS+ 74
Network Address Port Translation 134
Network Address Translation. See NAT
No Answer timer 279

no keyword 84

O

object access 61
off-hook test 246
On Hold timer 279
online comand help
debug commands 81
online command help 81
debug commands
debug
command help 88
general 81
interactive mode 82
maintenance commands 81, 86
specific 81
operations
monitoring tools 339
summary 323
outbound access prefix digit 258
over-contract region 184, 185

P

PABX connection
MGCP gateway 211
packet anomaly protection 141
packet capture (tcpdump) 352
packet loss 188
packet processing for security 129
parameter values 84
partitions 359
password
authentication 62, 65
changing 59
command 59
entry 58
security 57
pause frames 98
payload type
SIP gateway 225, 282
peak traffic 188
phone numbers, SIP endpoints 284
ping
command 355
DNS client 52
sweep protection 147
PMON 340
statistics 343
policies
firewall 130
GoS 191

IKE 155
IPsec 160
NAT 135
listing 139
policing methods 183
pools, DHCP 309
port
FxS configuration 238
LAN switch 97
VLAN assignment 111
WAN 91
mii0 91
speed 92
statistics 331
port forwarding 137
NAT 134
port mirroring 339
port scan protection 146
prefix digit 258
prefixes for commands 83
preshared key records 156
primary key for a command 82
priority queues
ARL 104
layer 2 QoS 107
prompt
changing 79
proposals, IPsec 160
protocol
connection 401
Transport Layer 401
user authentication 401
Protocol Monitoring. See PMON
proxy server 267
public addresses 136
public key upload for SSH 38
PuTTY 399

Q

QoS
disabled by ARL 104
flow control 98
LAN switch 106
layer 2. See Layer 2 QoS
layer 3 181
layer 3 configuration 185
layer 3 statistics 193
multi-service 31
quality group. See Quality group
voice traffic 181
quality group
audio 230

configuration 187
default (best effort) 188
definition 182
GoS security policy 192
listing 190
MGCP signaling traffic 217
SIP signaling traffic 273
traffic flow assignment 190
Quality of Service. See QoS
queuing mechanisms 107

R

RADIUS
flood protection 145
Radius
activity logs 71, 74
Radius client 68, 71
receiver off-hook test 246
redirection 134
reformatting memory command 361
register display 321
registrar domain, SIP phones 267
registration
MGCP endpoint status handling 220
MGCP endpoints 227
SIP endpoint listing 276
SIP endpoints 288
SIP expiration 277, 279
relay
DHCP 312
DNS 313
SNTP 315
TFTP 316
relay cache, DNS 314
remote administration 33
remote connection listing 34
REN test 247
reset timer 49
resistance tests 246
restart timer 49
retransmission timers
SIP 273
SIP gateway 279
reverse NAT 134
R-factor alarms 247
RFC compliance 411
rights settings 61
ringing cadences 239
RIP
definition 121
device support 126
flood protection 145

route listing 127
RIP daemon
starting 126
route configuration 124
route table listing 125
routing
static 124
VPN tunnel 163
routing configuration 121
routing daemon
definition 121
Routing Information Protocol. See RIP
RSA key 40
RSIP 211
RTP
attack protection 141
rules
firewall 130
rx port
MGCP 217
SIP 273
rx setting
FxO port 260
FxS port 243

S

sanity check 130
SAs 153
save command 79
saving the configuration 79
scan protection, IDS 146
scheduling methods, layer 2 QoS 107
SDP 264
Secure Shell. See SSH
Secure Socket Layer. See SSL
security
configuration 129
password 57
traffic processing 129
security associations 153
IKE 157
IPsec 162
security event logging 324
security policies
firewall 130
configuration 131
initial 130
listing 132
log entries 132
GoS
listing 193
GoS traffic flow assignment 191

self-signed certificate 43
serial number 323
server
DHCP 309
log destination 329
MGCP call server 212
Radius 68, 71
SIP call server
additional inbound 266
SSH 36
TACACS+ 74
telnet 34
web 38
service codes 285
session controller
MGCP 210, 215
SIP 264
Session Description Protocol 264
Session Initiation Protocol. See SIP
session logout 78
session timeout, command entry 79
Session-Expires parameters 279
SFTP session
to upload public key 38
shell commands 79
shipped configuration 53
silence suppression
SIP 225, 282
SIP
Access Control List 232
account authentication 281
additional inbound servers 266
Call Admission Control 236
call records 276
call server
profile 267
status 270
call statistics 275
ESH 277
flood protection 145
FXS port configuration 238
gateway 265
features 278
gateway configuration 280
Media Bridge 229
media connection statistics 231
phone registrar domain 267
proxy servers 266
session controller 264
status 274
signaling statistics 274
SSP 272
terminal accounts 264

user agent 265
SIP Signalling Proxy. See SSP
SIP/PSTN gateway 256
SNMP
community configuration 348
flood protection 145
traps 347, 351
SNMP agent 347
SNTP
configuration command 48
flood protection 145
relay 315
session listing 316
time acquisition 47
software upgrade procedures 362
speed
WAN port 92
spoof protection, IDS 147
SSH
authentication 36
client 36
internet access 401
key regeneration 37
server 36
server port 37
traffic security policy 36
SSH-AUTH 401
SSH-CONNECT 401
SSH-TRANS 401
SSL
certificate 42
certificate signing request 41
configuration example 43
CSR 41
upload 42
key 40
SSL CSR
upload 42
SSP 272
standard NAT 134
standards compliance 411
startup commands 80
static NAT 134
static NAT forwarding 138
static route
add 125, 126
delete 126
static routing
configuration 123
definition 121
statistics
call quality alarms 252
CDP 236

eth0 interface 94
Ethernet interfaces 331
GoS 193
cumulative 193
instantaneous 195
ICMP traffic 333
IDS 149
IKE 158
IP stack 331
IPsec 163
jitter buffer 240
LAN switch ports 100
log servers 330
media connections 231
MGCP
session controller calls 219
signaling 218
Netflow exporter activity 346
PMON traces 343
SIP call records 276
SIP calls 275
SIP signaling 274
SNMP agent 349
TCP traffic 335
UDP traffic 335
voice quality 250
voice quality detail 251
web server 40
status
media connections 230
strict policing 183
switch
configuration 97
features 97
port listing 99
statistics 100
VLAN ports 111
switch ports 97
SYN flood protection 144
Syslog
log server example 330
logging destination 327, 329
server 329
server messages 330
system
hardware 322
memory 323
module log 325
monitoring 321
operations summary 323

T

TACACS+
- client 74

tagging
- VLAN ID 112

TCP
- attack protection 141
- connection timeout 133
- statistics 335
- SYN scan protection 147

tcpdump command 352

telephone features
- MGCP 211
- SIP 265

telephony interfaces 31

Telnet
- access 34
- client 34
- command 35
- connection timeout 133
- port 35
- server 34
- session
  - example 35
  - start 35
- traffic security policy 34

Tera Term Pro 399

terminal emulator 32

terminal session settings 78

TFTP
- ALG support 140
- download files 318
- file cache 318
- flood protection 145
- relay 316
- session listing 317

time
- command 47
- display 47

time setting 47

timeout for command session 79

timeout for connections 133

tone configuration 241

tone settings 241

TOS field re-marking 31

traceroute command 356

tracing
- incoming traffic 340
- route across network 356

traffic
- best effort (QoS) 187
- contention 181

ICMP 333
IP stack 332
mirroring 339
security processing 129
TCP 335
trace 340
traffic flow
assignment to quality groups 190
traffic policing 183
traffic protection
ARP 191
VoIP 191
Transport Layer Protocol 401
tunnel interface 153
tx setting
FxO port 260
FxS port 243

U

UDP
attack protection 141
flood protection 143
log server 329
log server example 330
logging destination 327
port scan protection 146
statistics 335
unit name change 239
untagged packets 112
upgrading software 359
via Web UI 363
uplink
LAN port features 97
WAN port 91
user
accounts 61
configuration 61
active listing 60
rights settings 61
user agent
MGCP 211, 222
SIP 265
User Authentication Protocol 401
user groups 58, 61
user management
features 57
useradv rights 66
userbasic rights 66

V

VAD

SIP 225, 282
variable-length subnet masks 126
vid
VLAN 112
vif interface 114
virtual LAN. See VLAN
virtual private networks 153
VLAN 111
deletion 117
disabling 117
interface 114
port assignment 111
vid 112
VLSMs 126
voice
traffic protection 181, 191
Voice Activity Detection
SIP 225, 282
voice quality group 230
Voice Quality Monitoring analyser 247
voice tone configuration 241
VoIP
traffic protection 191
VoIP gateway 30
VoIP session controller
MGCP 209
SIP 263
voltage tests 245
VPN
configuration examples 163
support 153
vpn interface 161
VPN-A proposal 160
VQM analyser 247

W

WAN
VLAN 113
WAN port
statistics 94, 331
warmstart 347
watchdog reset timer 49
Web
traffic security policy 39
web server 38
statistics 40
Web UI
server configuration 38
Weighted Fair Queuing 107
WFQ 107
whoison command 34
width of terminal line 79

WinSCP3 399
wire speed 97

X

X509 CSR 41